Laxmi Ghanate (bnk2zk) | SYS 4050: Risk Analysis | April 26 2025

# Risk Analysis of AI-Driven Cybersecurity in Smart Home IoT Systems

# Executive Summary

- **Vision**: Empower smart homes with proactive cybersecurity by integrating AI-based risk analysis systems that monitor IoT devices, detect threats in real time, and adapt to evolving attack patterns.
- **Risk**: This report identifies critical risk categories—including device vulnerabilities, network exposure, user behavior, and system redundancy—analyzed using SEIRS models, fault trees, MCDA, and resilience curves to provide a layered defense framework for smart home IoT systems.
- **Deploy**: The proposed subtasks and deliverables guide deployment phases, supporting timely rollout of AI monitoring systems. Success will be measured by improved response time, reduction in residual risk, and increased user trust in smart home security infrastructure.

[1] https://doi.org/10.3390/electronics12183958
[2] https://doi.org/10.3389/fdata.2024.1402745

# Background

- IoT (Internet of Things) refers to everyday objects embedded with sensors, software, and connectivity to collect and exchange data [5].
- In smart homes, IoT includes:
  - Smart lighting, thermostats, door locks, refrigerators, voice assistants, etc. [5]
  - All devices are connected to the internet for automation and remote control.
- Adoption trends:
  - Over 57 million U.S. households used smart home devices by 2022, with continued growth [5].
- Security concerns:
  - Each connected device increases the home's cyber attack surface.
  - Many devices lack built-in security:
    - Default passwords
    - Weak or no encryption [1][2]
- Notable incidents
  - Mirai malware (2016): Hijacked consumer devices to launch massive botnet attacks [1].Smart thermostat hacks: Potential to cause physical harm if misused [2].
- Takeaway:
  - Smart home cybersecurity is about more than privacy: it's essential for protecting daily safety and reliability of household devices.

[1] https://doi.org/10.3390/electronics12183958
[2] https://doi.org/10.3389/fdata.2024.1402745
[5] https://www.oberlo.com/statistics/smart-home-statistics

# Motivation and Purpose

- **IoT growth is a double-edged sword**:
    - Brings convenience and innovation, but also rapidly introduces **new cybersecurity vulnerabilities** [2][3].
- **Current threat landscape:**
    - Rise in **IoT-targeted attacks**, such as:
        - Hackers accessing home networks via smart devices
        - Botnets exploiting poorly secured gadgets [1][2]
    - **Consumer concerns:** Privacy and security rank among top issues in adopting smart home tech [5].
    - **Organizational concerns:** Risk professionals list **IoT-related cyber threats** and privacy breaches as major priorities [2].
- **Client Context:**
    - **SmartSecure Systems**, a cybersecurity firm specializing in residential AI-based solutions, is seeking **an intelligent, scalable risk analysis approach**.
    - Their goal: Offer homeowners **real-time protection** from evolving threats with **minimal user intervention**.
- **Why AI is the solution:**
    - Traditional static defenses (e.g., checklists, rules-based systems) can't keep pace with:
        - The **scale**, **variety**, and **speed** of modern IoT environments [2][3].
    - AI excels at:
        - **Analyzing massive IoT data streams**
        - **Detecting subtle anomalies and threats**
        - **Learning and adapting continuously** to new attack patterns [3][2]
- **Bottom line:**
    - AI-driven risk analysis acts as an **automated watchdog**, proactively securing smart homes by **foreseeing and mitigating threats** before they escalate.

[1] https://doi.org/10.3390/electronics12183958
[2] https://doi.org/10.3389/fdata.2024.1402745
[3] https://doi.org/10.3390/brainsci13040683
[5] https://www.oberlo.com/statistics/smart-home-statistics

# Problem Statement

- Despite the growing awareness of IoT security issues, current approaches to cybersecurity risk analysis often fall short in smart home environments. One fundamental challenge is the sheer diversity and complexity of IoT devices – a typical smart home might have gadgets from dozens of manufacturers, each with different hardware, software, and communication protocols.

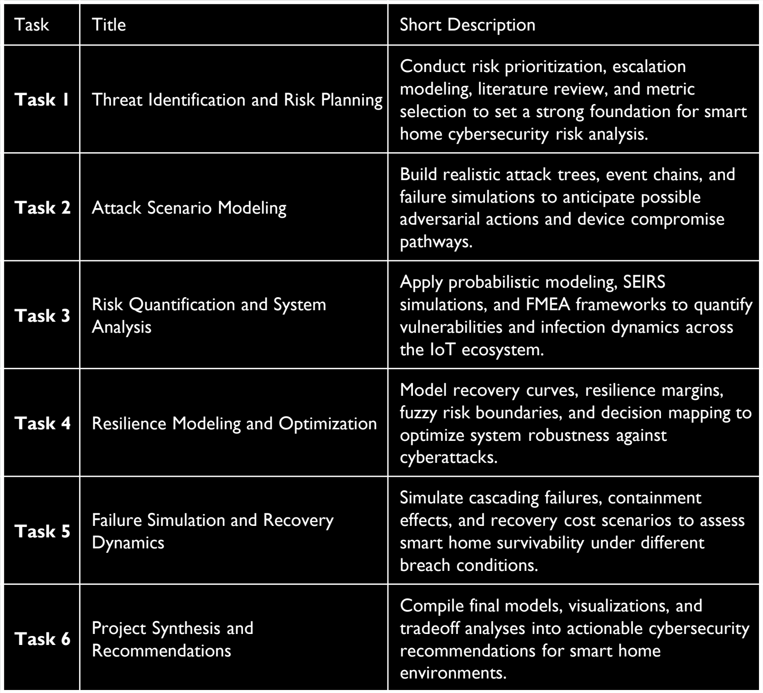
- Conventional risk assessment models struggle to account for this heterogeneity and the intricate ways these devices interconnect and depend on each other [2][4]. Many legacy security tools lack real-time adaptability; they cannot dynamically adjust to new devices being added or novel attack patterns being developed by threat actors [2][4].

- Furthermore, the IoT domain suffers from a dearth of historical data and standardized metrics for quantifying cyber risk. In traditional IT networks, risk is often evaluated as a function of likelihood and impact, but in IoT, we lack reliable statistics on how likely certain attacks are or what their potential impact could be [5]. This makes it difficult for stakeholders to prioritize investments and responses effectively. Additionally, there are currently no universally adopted standards or regulations specifically guiding IoT risk assessments for home devices, leading to inconsistent security measures across different products and brands [5]. The crux of the problem is clear – we need new risk analysis techniques capable of operating in a highly distributed, diverse, and evolving environment, where traditional cybersecurity paradigms are not sufficient to ensure protection [2][3].

[2] https://doi.org/10.3389/fdata.2024.1402745
[4] https://doi.org/10.3390/s22052017
[5] https://www.oberlo.com/statistics/smart-home-statistics

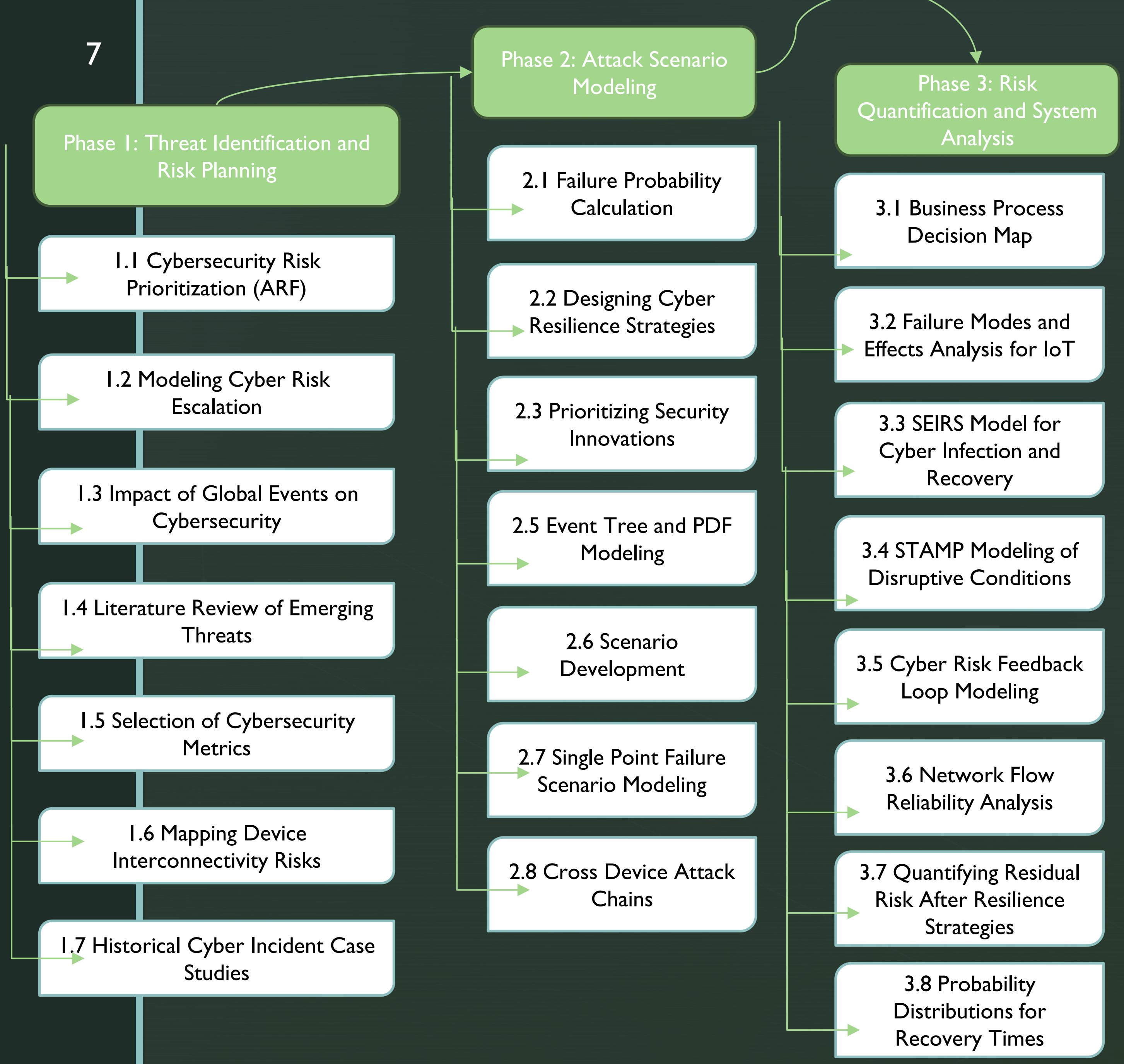
# Methodology

This project will perform six structured tasks for the risk analysis of cybersecurity threats in AI-powered smart home IoT environments. Each task logically groups several modeling, simulation, or planning activities, most of which have been partially or fully developed during prior assignments and course readings.



| Task | Title | Short Description |
|---|---|---|
| **Task 1** | Threat Identification and Risk Planning | Conduct risk prioritization, escalation modeling, literature review, and metric selection to set a strong foundation for smart home cybersecurity risk analysis. |
| **Task 2** | Attack Scenario Modeling | Build realistic attack trees, event chains, and failure simulations to anticipate possible adversarial actions and device compromise pathways. |
| **Task 3** | Risk Quantification and System Analysis | Apply probabilistic modeling, SEIRS simulations, and FMEA frameworks to quantify vulnerabilities and infection dynamics across the IoT ecosystem. |
| **Task 4** | Resilience Modeling and Optimization | Model recovery curves, resilience margins, fuzzy risk boundaries, and decision mapping to optimize system robustness against cyberattacks. |
| **Task 5** | Failure Simulation and Recovery Dynamics | Simulate cascading failures, containment effects, and recovery cost scenarios to assess smart home survivability under different breach conditions. |
| **Task 6** | Project Synthesis and Recommendations | Compile final models, visualizations, and tradeoff analyses into actionable cybersecurity recommendations for smart home environments. |

# Flowchart



## Phase 1: Threat Identification and Risk Planning

- 1.1 Cybersecurity Risk Prioritization (ARF)
- 1.2 Modeling Cyber Risk Escalation
- 1.3 Impact of Global Events on Cybersecurity
- 1.4 Literature Review of Emerging Threats
- 1.5 Selection of Cybersecurity Metrics
- 1.6 Mapping Device Interconnectivity Risks
- 1.7 Historical Cyber Incident Case Studies

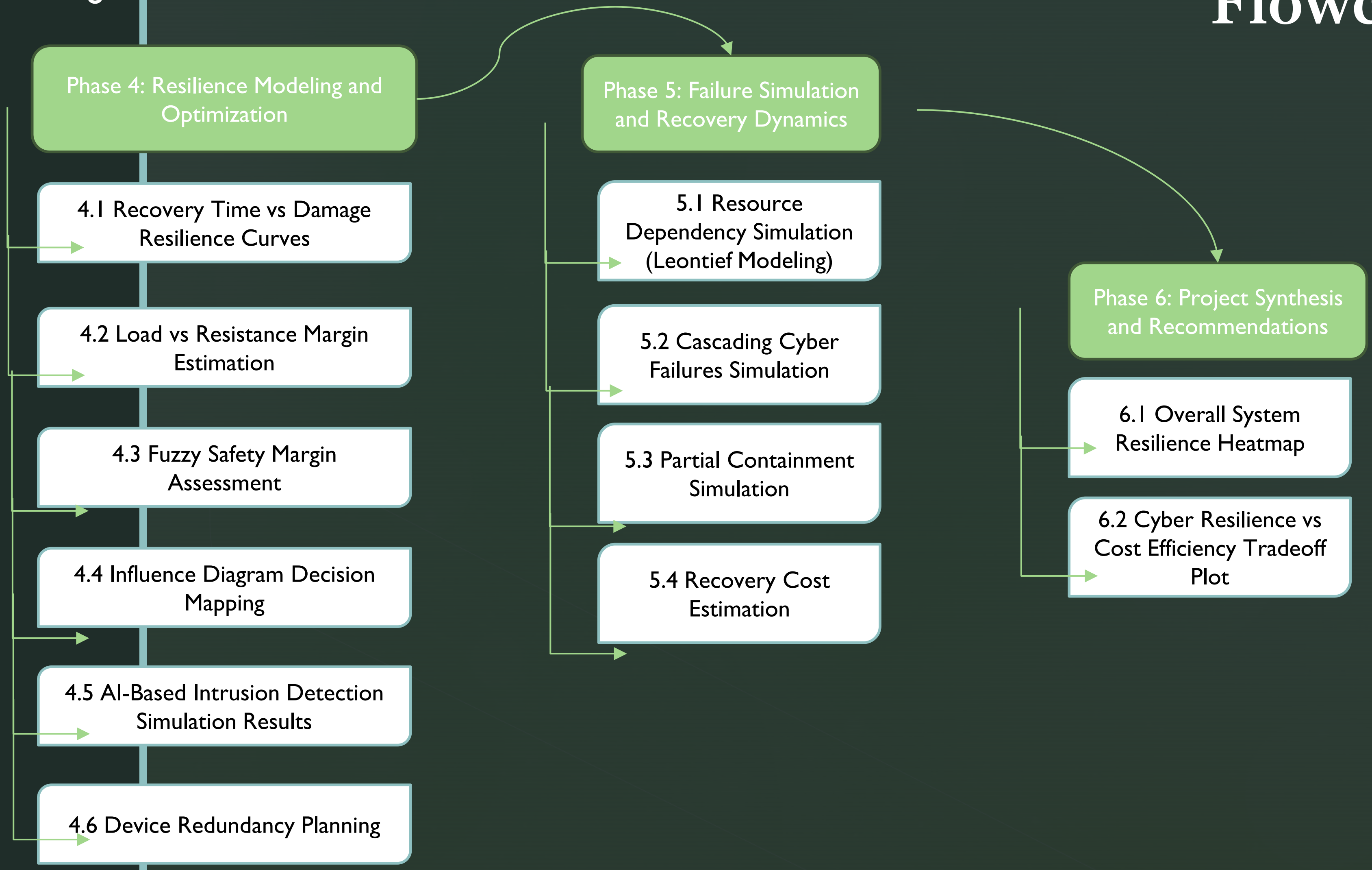
## Phase 2: Attack Scenario Modeling

- 2.1 Failure Probability Calculation
- 2.2 Designing Cyber Resilience Strategies
- 2.3 Prioritizing Security Innovations
- 2.5 Event Tree and PDF Modeling
- 2.6 Scenario Development
- 2.7 Single Point Failure Scenario Modeling
- 2.8 Cross Device Attack Chains

## Phase 3: Risk Quantification and System Analysis

- 3.1 Business Process Decision Map
- 3.2 Failure Modes and Effects Analysis for IoT
- 3.3 SEIRS Model for Cyber Infection and Recovery
- 3.4 STAMP Modeling of Disruptive Conditions
- 3.5 Cyber Risk Feedback Loop Modeling
- 3.6 Network Flow Reliability Analysis
- 3.7 Quantifying Residual Risk After Resilience Strategies
- 3.8 Probability Distributions for Recovery Times

# Flowchart



Phase 4: Resilience Modeling and Optimization

4.1 Recovery Time vs Damage Resilience Curves

4.2 Load vs Resistance Margin Estimation

4.3 Fuzzy Safety Margin Assessment

4.4 Influence Diagram Decision Mapping

4.5 AI-Based Intrusion Detection Simulation Results

4.6 Device Redundancy Planning

Phase 5: Failure Simulation and Recovery Dynamics

5.1 Resource Dependency Simulation (Leontief Modeling)

5.2 Cascading Cyber Failures Simulation

5.3 Partial Containment Simulation

5.4 Recovery Cost Estimation

Phase 6: Project Synthesis and Recommendations

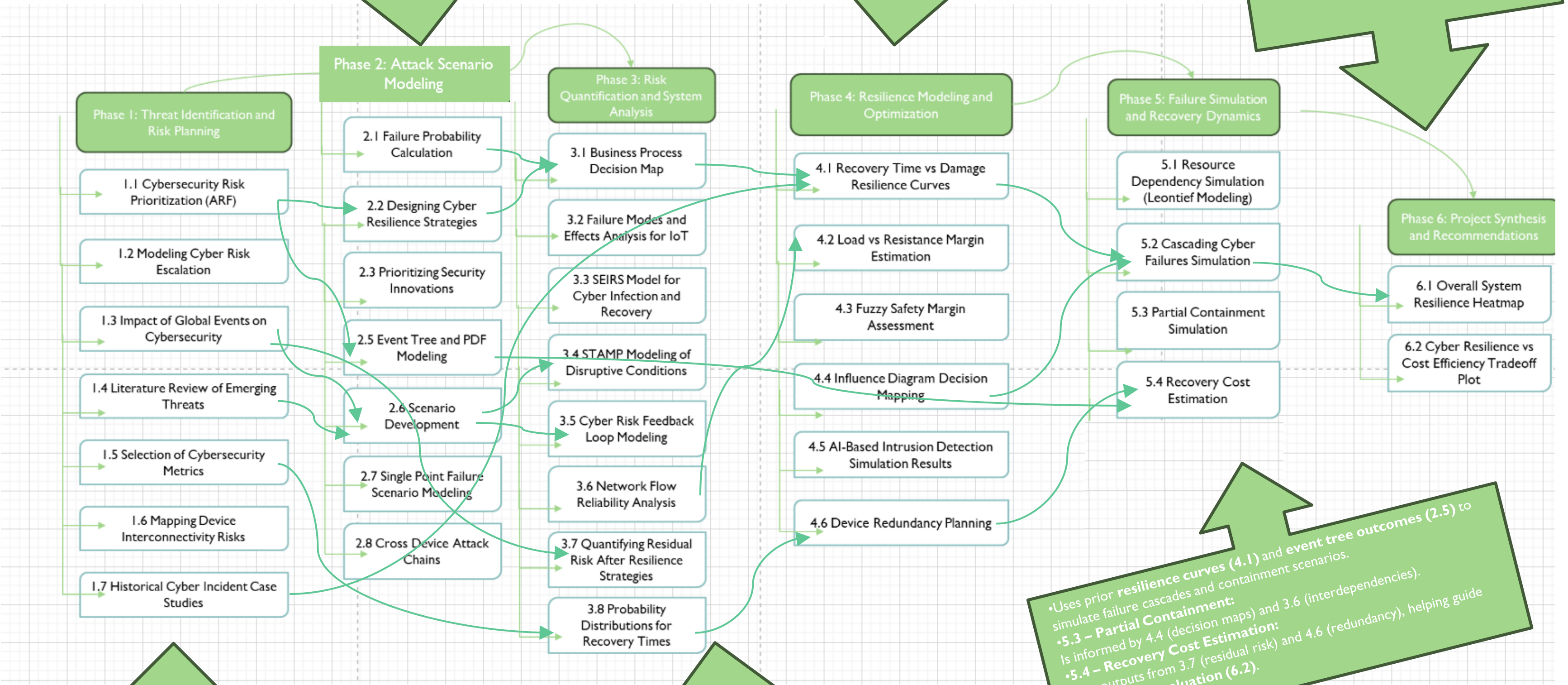
6.1 Overall System Resilience Heatmap

6.2 Cyber Resilience vs Cost Efficiency Tradeoff Plot

**•2.1 to 2.3 – Risk Modeling, SEIRS, Prioritization:**
Directly inform **MCDA analysis** (3.1, 3.2), **event tree construction (2.5)**, and **feedback loops (3.5)**.
**•2.5 – Event Tree and PDF Modeling:**
This task feeds into **Phase 3's probabilistic modeling** (3.8) and **resilience assessments (4.1, 4.2)**.
**•2.6–2.8 – Scenario Modeling:**
These simulate single-point and cross-device failure conditions, **providing the pathways** that shape **failure mode analysis (3.2)** and **STAMP modeling (3.4)**.

**•4.1 – Damage vs Recovery Curves:**
Fed by failure and disruption models (3.2, 3.4). Output goes into 5.2 and 5.4.
**•4.4 – Influence Diagram:**
Maps decision logic and feeds **5.3 (containment simulation)**.
**•4.6 – Device Redundancy Planning:**
Derived from dependency modeling (3.6) and helps define **resilience margin (4.2)** and **recovery paths (5.2)**.

**•6.1 – Resilience Heatmap:**
Synthesizes all resilience indicators from 3.7, 4.1, and 5.2.
**•6.2 – Cost Efficiency Tradeoff Plot:**
Uses data from 5.4 and MCDA from 2.3 to evaluate best-fit solutions.



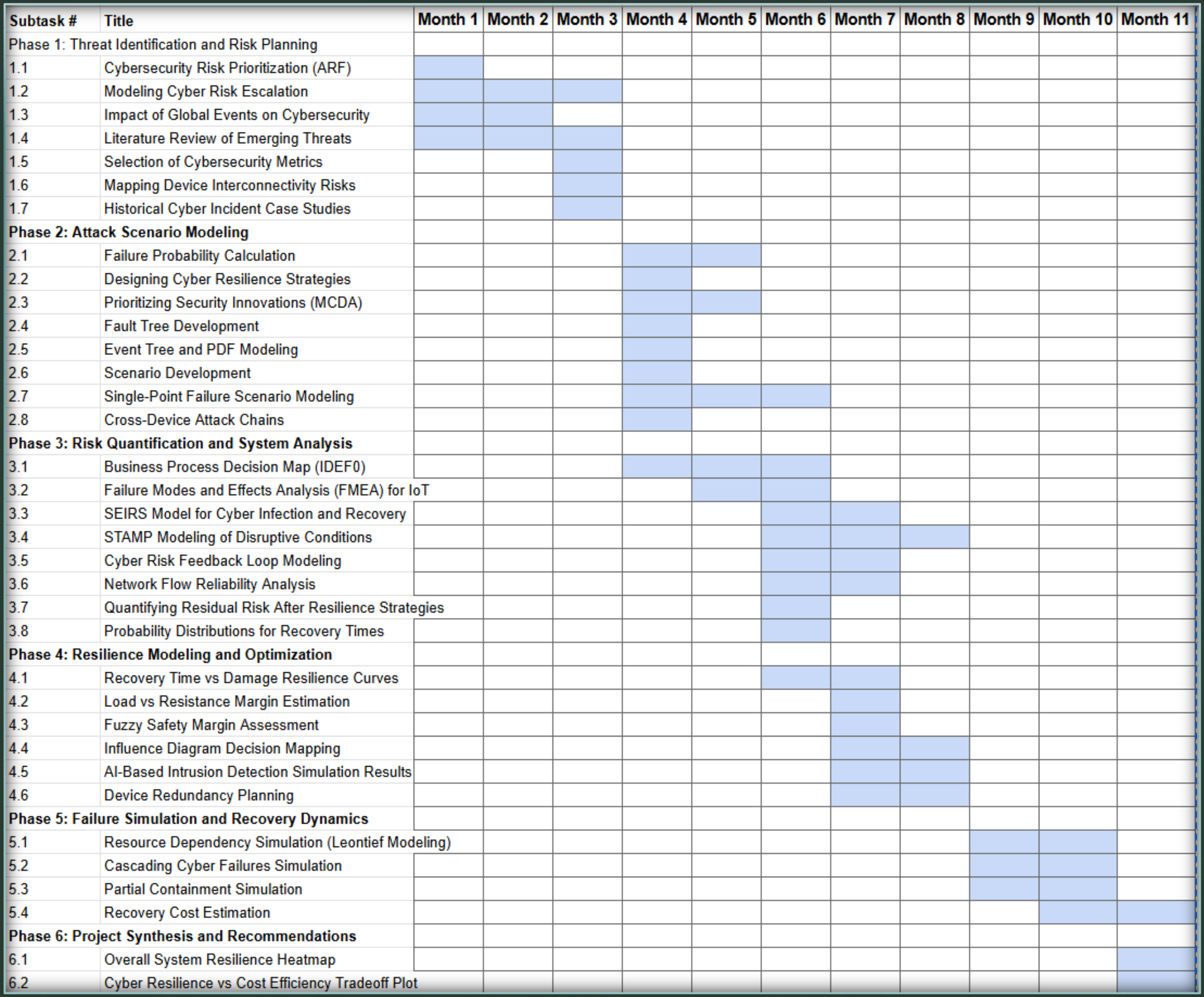
Phase 1: Threat Identification and Risk Planning
1.1 Cybersecurity Risk Prioritization (ARF)
1.2 Modeling Cyber Risk Escalation
1.3 Impact of Global Events on Cybersecurity
1.4 Literature Review of Emerging Threats
1.5 Selection of Cybersecurity Metrics
1.6 Mapping Device Interconnectivity Risks
1.7 Historical Cyber Incident Case Studies
Phase 2: Attack Scenario Modeling
2.1 Failure Probability Calculation
2.2 Designing Cyber Resilience Strategies
2.3 Prioritizing Security Innovations
2.5 Event Tree and PDF Modeling
2.6 Scenario Development
2.7 Single Point Failure Scenario Modeling
2.8 Cross Device Attack Chains
Phase 3: Risk Quantification and System Analysis
3.1 Business Process Decision Map
3.2 Failure Modes and Effects Analysis for IoT
3.3 SEIRS Model for Cyber Infection and Recovery
3.4 STAMP Modeling of Disruptive Conditions
3.5 Cyber Risk Feedback Loop Modeling
3.6 Network Flow Reliability Analysis
3.7 Quantifying Residual Risk After Resilience Strategies
3.8 Probability Distributions for Recovery Times
Phase 4: Resilience Modeling and Optimization
4.1 Recovery Time vs Damage Resilience Curves
4.2 Load vs Resistance Margin Estimation
4.3 Fuzzy Safety Margin Assessment
4.4 Influence Diagram Decision Mapping
4.5 AI-Based Intrusion Detection Simulation Results
4.6 Device Redundancy Planning
Phase 5: Failure Simulation and Recovery Dynamics
5.1 Resource Dependency Simulation (Leontief Modeling)
5.2 Cascading Cyber Failures Simulation
5.3 Partial Containment Simulation
5.4 Recovery Cost Estimation
Phase 6: Project Synthesis and Recommendations
6.1 Overall System Resilience Heatmap
6.2 Cyber Resilience vs Cost Efficiency Tradeoff Plot

•Uses prior **resilience curves (4.1)** and **event tree outcomes (2.5)** to simulate failure cascades and containment scenarios.
**•5.3 – Partial Containment:**
Is informed by 4.4 (decision maps) and 3.6 (interdependencies).
**•5.4 – Recovery Cost Estimation:**
Uses outputs from 3.7 (residual risk) and 4.6 (redundancy), helping guide **cost-benefit evaluation (6.2)**.

**•1.1 – ARF (Cybersecurity Risk Prioritization):**
Feeds into nearly all of Phase 2 because it ranks which risks to analyze and simulate first.
**•1.3 – Impact of Global Events** and **1.7 – Historical Case Studies:**
Provide **real-world scenarios and disruption patterns** that shape scenario models (2.6–2.8) and inform **STAMP modeling (3.4)** and **resilience simulations (5.2)**.
**•1.5 and 1.6 – Metrics and Device Mapping:**
Feed into 2.1, 2.7, and especially 3.6 (network reliability) and 3.5 (feedback loops).

**•3.2 – FMEA for IoT:**
Uses outputs from 2.1, 2.7, and 2.8 to model failure points and flows into 4.1 (resilience) and 5.2 (simulation).
**•3.3 – SEIRS Model:**
Refines the dynamic modeling from 2.3 and feeds 3.7 (residual risk) and 4.4 (influence diagram).
**•3.5 – Feedback Loop Modeling:**
Relates to **AI-based intrusion detection** and **dynamic threat response** (4.5).
**•3.7 – Quantifying Residual Risk:**
Summarizes performance impacts **after resilience strategies** and flows into **cost estimation (5.4)** and **system heatmap (6.1)**.

# Gantt Chart



| Subtask # | Title | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 | Month 9 | Month 10 | Month 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phase 1: Threat Identification and Risk Planning | | | | | | | | | | | | |
| 1.1 | Cybersecurity Risk Prioritization (ARF) | 🟦 | | | | | | | | | | |
| 1.2 | Modeling Cyber Risk Escalation | 🟦 | 🟦 | 🟦 | | | | | | | | |
| 1.3 | Impact of Global Events on Cybersecurity | 🟦 | 🟦 | | | | | | | | | |
| 1.4 | Literature Review of Emerging Threats | 🟦 | 🟦 | 🟦 | | | | | | | | |
| 1.5 | Selection of Cybersecurity Metrics | | | 🟦 | | | | | | | | |
| 1.6 | Mapping Device Interconnectivity Risks | | | 🟦 | | | | | | | | |
| 1.7 | Historical Cyber Incident Case Studies | | | 🟦 | | | | | | | | |
| **Phase 2: Attack Scenario Modeling** | | | | | | | | | | | | |
| 2.1 | Failure Probability Calculation | | | | 🟦 | 🟦 | | | | | | |
| 2.2 | Designing Cyber Resilience Strategies | | | | 🟦 | | | | | | | |
| 2.3 | Prioritizing Security Innovations (MCDA) | | | | 🟦 | 🟦 | | | | | | |
| 2.4 | Fault Tree Development | | | | 🟦 | | | | | | | |
| 2.5 | Event Tree and PDF Modeling | | | | 🟦 | | | | | | | |
| 2.6 | Scenario Development | | | | 🟦 | | | | | | | |
| 2.7 | Single-Point Failure Scenario Modeling | | | | 🟦 | 🟦 | 🟦 | | | | | |
| 2.8 | Cross-Device Attack Chains | | | | 🟦 | | | | | | | |
| **Phase 3: Risk Quantification and System Analysis** | | | | | | | | | | | | |
| 3.1 | Business Process Decision Map (IDEF0) | | | | 🟦 | 🟦 | 🟦 | | | | | |
| 3.2 | Failure Modes and Effects Analysis (FMEA) for IoT | | | | | 🟦 | 🟦 | | | | | |
| 3.3 | SEIRS Model for Cyber Infection and Recovery | | | | | | 🟦 | 🟦 | | | | |
| 3.4 | STAMP Modeling of Disruptive Conditions | | | | | | 🟦 | 🟦 | 🟦 | | | |
| 3.5 | Cyber Risk Feedback Loop Modeling | | | | | | 🟦 | 🟦 | | | | |
| 3.6 | Network Flow Reliability Analysis | | | | | | 🟦 | 🟦 | | | | |
| 3.7 | Quantifying Residual Risk After Resilience Strategies | | | | | | 🟦 | | | | | |
| 3.8 | Probability Distributions for Recovery Times | | | | | | 🟦 | | | | | |
| **Phase 4: Resilience Modeling and Optimization** | | | | | | | | | | | | |
| 4.1 | Recovery Time vs Damage Resilience Curves | | | | | | 🟦 | 🟦 | | | | |
| 4.2 | Load vs Resistance Margin Estimation | | | | | | | 🟦 | | | | |
| 4.3 | Fuzzy Safety Margin Assessment | | | | | | | 🟦 | | | | |
| 4.4 | Influence Diagram Decision Mapping | | | | | | | 🟦 | 🟦 | | | |
| 4.5 | AI-Based Intrusion Detection Simulation Results | | | | | | | 🟦 | 🟦 | | | |
| 4.6 | Device Redundancy Planning | | | | | | | 🟦 | 🟦 | | | |
| **Phase 5: Failure Simulation and Recovery Dynamics** | | | | | | | | | | | | |
| 5.1 | Resource Dependency Simulation (Leontief Modeling) | | | | | | | | | 🟦 | 🟦 | |
| 5.2 | Cascading Cyber Failures Simulation | | | | | | | | | 🟦 | 🟦 | |
| 5.3 | Partial Containment Simulation | | | | | | | | | 🟦 | 🟦 | |
| 5.4 | Recovery Cost Estimation | | | | | | | | | | 🟦 | 🟦 |
| **Phase 6: Project Synthesis and Recommendations** | | | | | | | | | | | | |
| 6.1 | Overall System Resilience Heatmap | | | | | | | | | | | 🟦 |
| 6.2 | Cyber Resilience vs Cost Efficiency Tradeoff Plot | | | | | | | | | | | 🟦 |

## Threat Identification and Risk Planning

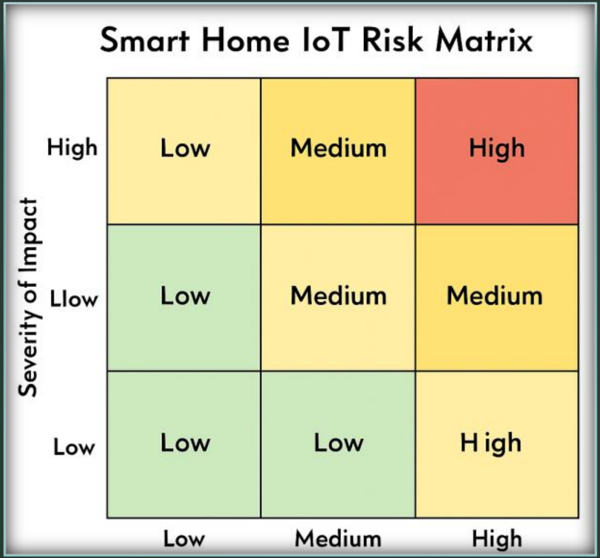
# Task 1

# 1.1: Cybersecurity Risk Prioritization via ARF

**This subtask will** prioritize cybersecurity threats in smart home IoT environments using Accident Reduction Factors (ARF) modeling. By assessing each device's likelihood of attack and the severity of potential consequences, this subtask will enable ranking of threats based on risk priority scores. High-risk devices such as smart locks and home security cameras will be given greater focus compared to lower-impact devices like smart lights.

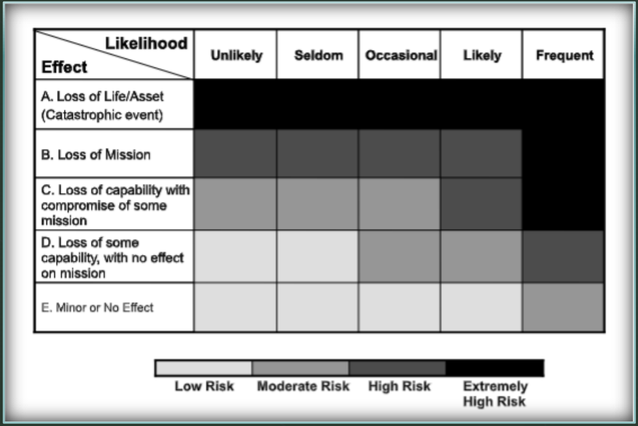
**The elements of this subtask are** assigning likelihood percentages, categorizing severity levels, and calculating risk priority numbers (RPNs) for each device type.

**The deliverables of this subtask are** a risk matrix table that maps smart home IoT threats based on their ARF-derived scores.



Smart Home IoT Risk Matrix

| Severity of Impact | | | |
|---|---|---|---|
| High | Low | Medium | High |
| Llow | Low | Medium | Medium |
| Low | Low | Low | H igh |
| | Low | Medium | High |

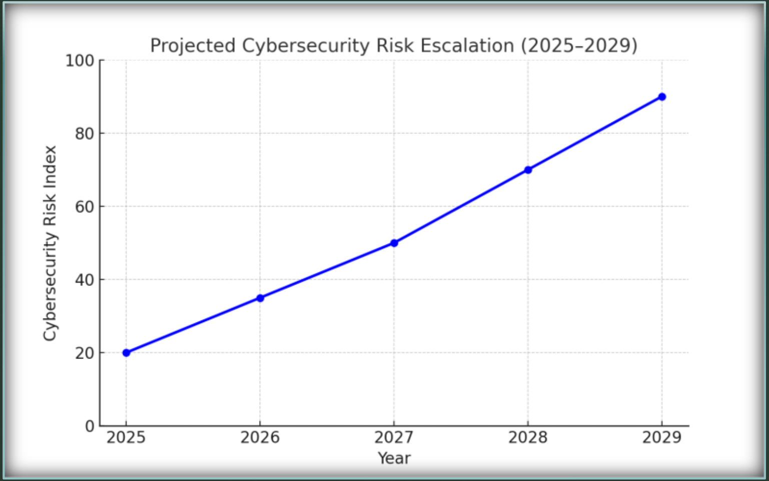


| Likelihood<br>Effect | Unlikely | Seldom | Occasional | Likely | Frequent |
|---|---|---|---|---|---|
| A. Loss of Life/Asset (Catastrophic event) | █ | █ | █ | █ | █ |
| B. Loss of Mission | ▓ | ▓ | ▓ | ▓ | █ |
| C. Loss of capability with compromise of some mission | ▒ | ▒ | ▒ | ▓ | █ |
| D. Loss of some capability, with no effect on mission | ░ | ░ | ▒ | ▒ | ▓ |
| E. Minor or No Effect | ░ | ░ | ░ | ░ | ▒ |

░ Low Risk ▒ Moderate Risk ▓ High Risk █ Extremely High Risk

# 1.2: Modeling Cyber Risk Escalation

**This subtask will** model the escalation of cybersecurity risks in smart homes over time, considering trends such as increasing device interconnectivity, adversarial AI developments, and the spread of malware. Future attack scenarios will be projected to better understand risk growth.
**The elements of this subtask are** gathering historical cyber incident data, projecting future attack trends, and plotting escalation curves for smart home vulnerabilities.
**The deliverables of this subtask are** a projected risk escalation graph showing expected growth in cybersecurity threats over a five-year horizon.



# 1.3: Impact of Global Events on Cybersecurity

**This subtask will** analyze how global events like new legislation, geopolitical cyber conflicts, or supply chain disruptions impact cybersecurity risks within smart homes. Special attention will be paid to events that influence device vulnerabilities or user trust.

**The elements of this subtask are** identifying relevant global events, mapping each event to its cyber risk implications, and assessing impact severity.

**The deliverables of this subtask are** a table matching key global events to specific risk shifts affecting smart home IoT systems.

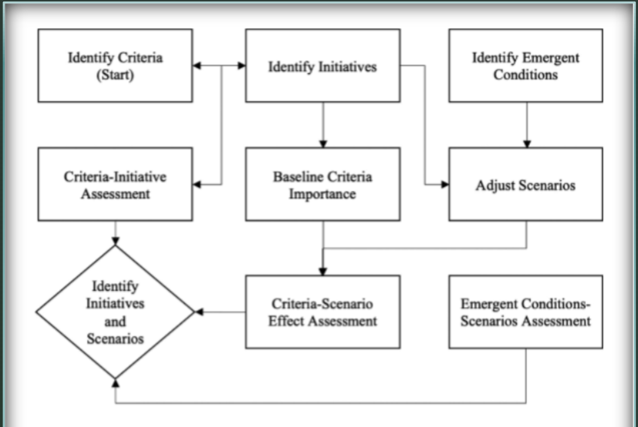
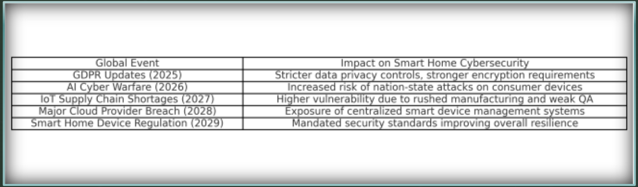

Identify Criteria (Start)
Identify Initiatives
Identify Emergent Conditions
Criteria-Initiative Assessment
Baseline Criteria Importance
Adjust Scenarios
Identify Initiatives and Scenarios
Criteria-Scenario Effect Assessment
Emergent Conditions-Scenarios Assessment

Fig. 1. Conceptual diagram of risk assessment methodology for hardware supply chains of charging infrastructure of electric vehicles.



| Global Event | Impact on Smart Home Cybersecurity |
|---|---|
| GDPR Updates (2025) | Stricter data privacy controls, stronger encryption requirements |
| AI Cyber Warfare (2026) | Increased risk of nation-state attacks on consumer devices |
| IoT Supply Chain Shortages (2027) | Higher vulnerability due to rushed manufacturing and weak QA |
| Major Cloud Provider Breach (2028) | Exposure of centralized smart device management systems |
| Smart Home Device Regulation (2029) | Mandated security standards improving overall resilience |

# 1.4: Literature Review of Emerging IoT Cybersecurity Threats

**This subtask will** conduct a focused literature review of the newest academic research and industry whitepapers (published within the past 3 years) related to cybersecurity threats in smart home IoT systems. This review will identify emerging attack trends (e.g., adversarial AI, side-channel attacks, firmware hijacking) that are not fully addressed by traditional security models.

**The elements of this subtask are** gathering 8–10 recent sources, summarizing emerging attack vectors and vulnerabilities, highlighting trends not widely mitigated yet, and mapping how these influence risk analysis planning.

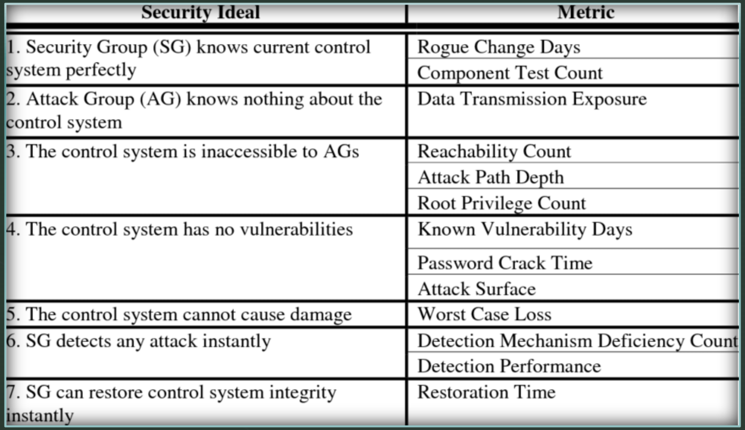
**The deliverable of this subtask is** a **Summary Table of Emerging Threats** organized by attack type, device target, and year/trend observed.

# 1.5: Selection of Cybersecurity Metrics for Risk Quantification

**This subtask will** select key cybersecurity metrics that will be used throughout the project to consistently quantify and compare risk levels across devices and systems. Metrics might include mean time to compromise (MTTC), mean time to detection (MTTD), severity scales, recovery rates, and attack success probabilities.

**The elements of this subtask are** reviewing standard cybersecurity KPIs (key performance indicators), adapting them for smart home IoT contexts, selecting a minimal set of primary metrics, and defining each metric's calculation method.

**The deliverable of this subtask is** a **Cybersecurity Metrics Table** listing selected risk quantification metrics, their definitions, and intended use in analysis models.



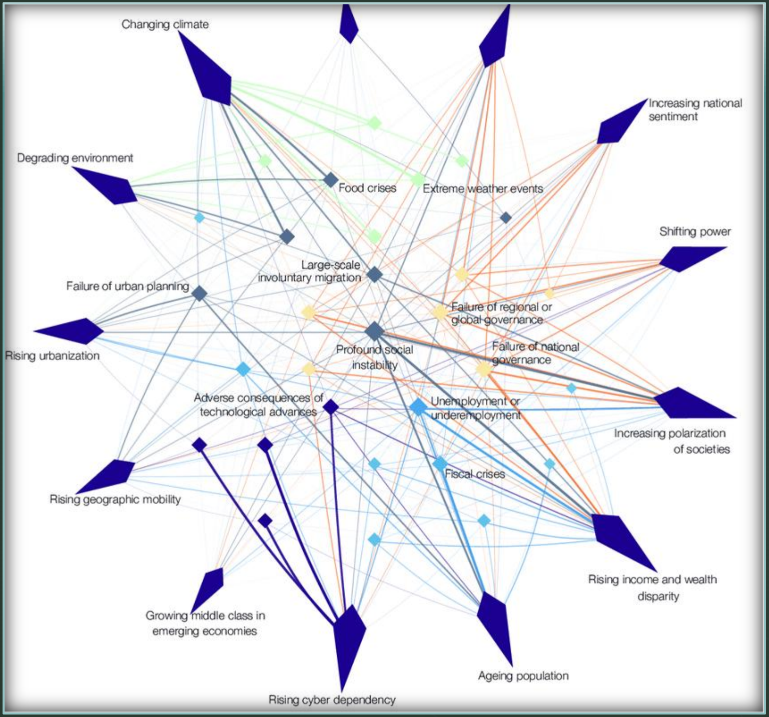
| Security Ideal | Metric |
|---|---|
| 1. Security Group (SG) knows current control system perfectly | Rogue Change Days |
| | Component Test Count |
| 2. Attack Group (AG) knows nothing about the control system | Data Transmission Exposure |
| 3. The control system is inaccessible to AGs | Reachability Count |
| | Attack Path Depth |
| | Root Privilege Count |
| 4. The control system has no vulnerabilities | Known Vulnerability Days |
| | Password Crack Time |
| | Attack Surface |
| 5. The control system cannot cause damage | Worst Case Loss |
| 6. SG detects any attack instantly | Detection Mechanism Deficiency Count |
| | Detection Performance |
| 7. SG can restore control system integrity instantly | Restoration Time |

# 1.6 – Mapping Device Interconnectivity Risks

**This subtask will** map the interconnectivity of smart home IoT devices to identify how compromises in one device could escalate across others. Focus will be on visualizing attack pathways between devices that communicate frequently (e.g., hubs, locks, cameras).

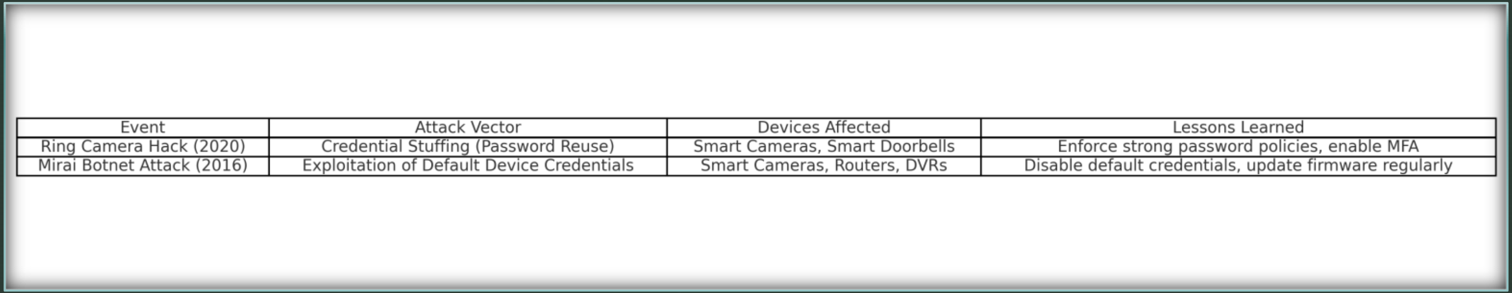
**The elements of this subtask are** mapping device communication dependencies, identifying critical nodes, and flagging high-risk pathways for propagation.

**The deliverable of this subtask is** a **Device Interconnection Risk Map**.


Changing climate
Increasing national sentiment
Degrading environment
Food crises
Extreme weather events
Shifting power
Large-scale involuntary migration
Failure of urban planning
Failure of regional or global governance
Profound social instability
Failure of national governance
Rising urbanization
Adverse consequences of technological advances
Unemployment or underemployment
Increasing polarization of societies
Rising geographic mobility
Fiscal crises
Rising income and wealth disparity
Growing middle class in emerging economies
Ageing population
Rising cyber dependency

https://www.researchgate.net/figure/THE-RISKS-TRENDS-INTERCONNECTIONS-MAP-2018_fig2_324691018

## 1.7 – Historical Cyber Incident Case Studies



| Event | Attack Vector | Devices Affected | Lessons Learned |
|---|---|---|---|
| Ring Camera Hack (2020) | Credential Stuffing (Password Reuse) | Smart Cameras, Smart Doorbells | Enforce strong password policies, enable MFA |
| Mirai Botnet Attack (2016) | Exploitation of Default Device Credentials | Smart Cameras, Routers, DVRs | Disable default credentials, update firmware regularly |

**This subtask will** summarize two recent real-world smart home cybersecurity breaches, analyzing how attackers succeeded and which devices were most vulnerable. Case study insights will guide later risk modeling.
**The elements of this subtask are** selecting 2 breach examples, mapping attack vectors, identifying failure points, and noting missed defenses.
**The deliverable of this subtask is** a **Cyber Incident Case Study Summary Table**.

Attack Scenario Modeling

# Task 2

# 2.1 – Failure Probability Calculation

**This subtask will** estimate the probability of failure for critical smart home IoT devices under targeted cybersecurity attacks. Using conditional probability models, this subtask will simulate different threat scenarios (e.g., device takeover via weak credentials, malware infection via outdated firmware) and calculate the chance of individual device failures leading to broader system compromise. The probability results will guide prioritization of defensive measures.

**The elements of this subtask are** defining possible attack events per device, assigning initial attack probabilities based on severity and frequency, calculating conditional failure probabilities depending on device states (compromised vs isolated), and summarizing results in a structured table.

**The deliverable of this subtask is** a **Probability Table** listing each device, potential attack types, and associated failure probabilities under different threat conditions.

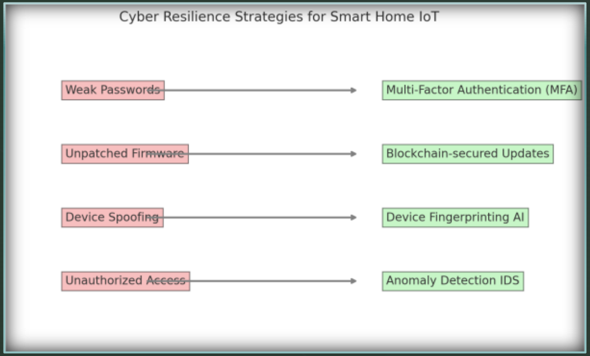
| Device | Threat Type | Probability of Attack (%) | Probability of Failure After Attack (%) |
|---|---|---|---|
| Smart Lock | Credential Theft | 20% | 70% |
| Smart Camera | Malware Infection | 15% | 60% |
| Smart Thermostat | Remote Code Injection | 10% | 50% |
| Smart Lightbulb | Network Snooping | 5% | 20% |
| Smart Hub | Man-in-the-Middle Attack | 25% | 80% |

# 2.2 – Designing Cyber Resilience Strategies

**This subtask will** design resilience strategies to mitigate high-risk vulnerabilities identified in the smart home IoT ecosystem. Emphasis will be placed on using advanced technologies such as AI-driven intrusion detection systems (IDS), multi-factor authentication (MFA), blockchain-secured firmware updates, and redundant fail-safe designs. Strategies will be mapped to specific device vulnerabilities and attack paths identified earlier.

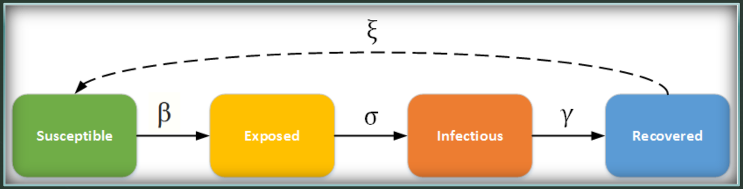
**The elements of this subtask are** selecting appropriate cybersecurity technologies, matching technologies to specific device or system weaknesses, designing fallback procedures for resilience (e.g., automatic quarantine of suspicious devices), and visually mapping the resilience structure.

**The deliverable of this subtask is** a **Cyber Resilience Strategy Diagram** connecting threats to specific mitigation technologies across the smart home system.



# 2.3 – SEIRS Model for Cyber Infection and Recovery

**This subtask will** prioritize proposed cybersecurity technologies using Multi-Criteria Decision Analysis (MCDA), balancing factors like effectiveness, cost, ease of implementation, and long-term maintainability. Each technology will be evaluated across weighted criteria, and the results will be ranked to guide which solutions should be deployed first.
**The elements of this subtask are** defining evaluation criteria (effectiveness, cost, feasibility, user impact), assigning weightings to each criterion based on project priorities, scoring each technology, and visually displaying comparative rankings.
**The deliverable of this subtask is** an **MCDA Table and/or Radar Chart** showing the relative priority of cybersecurity innovations for smart homes.



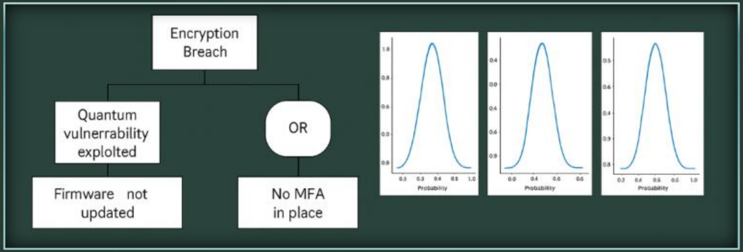
https://docs.idmod.org/projects/emod-hiv/en/2.20_a/model-seir.html

# 2.4 – Fault Tree and PDF Modeling

**This subtask will** develop fault trees to model how cyber failures can occur within a smart home IoT network, and generate corresponding probability density functions (PDFs) to quantify the likelihood of various failure paths. By visually tracing the root causes of security breaches, this subtask supports better preventative strategy design.

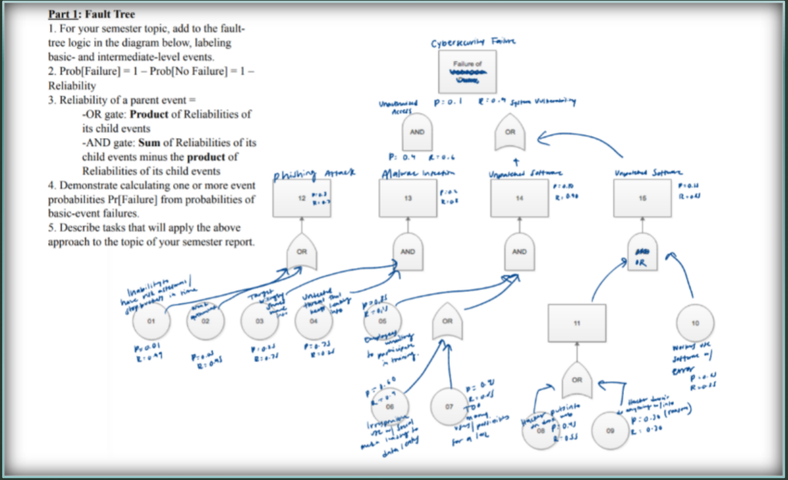
**The elements of this subtask are** identifying root causes of IoT failures, mapping failure sequences into a fault tree structure, calculating probabilities for different fault branches, and building probability density functions based on simulated failure data.

**The deliverables of this subtask are** a detailed fault tree diagram showing device compromise pathways, along with PDFs estimating the probability distributions of different failure outcomes.



# 2.5 – Event Tree and PDF Modeling

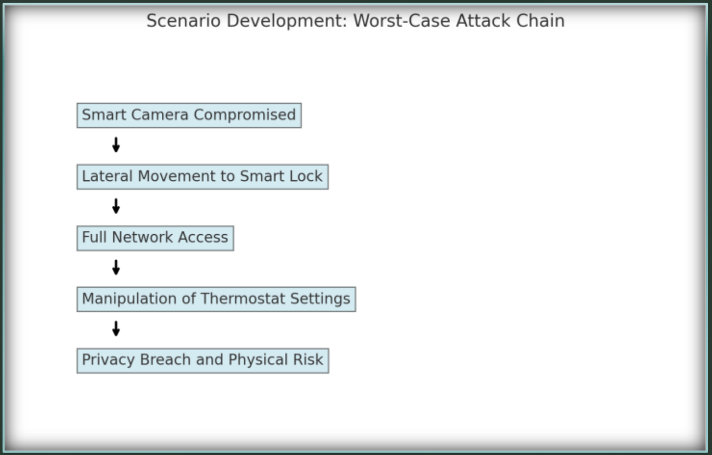
**This subtask will** create an event tree modeling the possible outcomes following a detected or undetected cybersecurity breach in the smart home, and generate probability density functions (PDFs) to estimate the likelihoods of different cascading events (e.g., minor breach contained vs full network compromise).
**The elements of this subtask are** defining initial breach events (detection or non-detection), mapping branching outcome sequences (containment, escalation, recovery), calculating branch probabilities, and fitting probability density functions to the event outcomes.
**The deliverable of this subtask is** an **Event Tree Diagram** with corresponding **Probability Density Function Graphs** for smart home cyber breaches.



**Part 1: Fault Tree**

1. For your semester topic, add to the fault-tree logic in the diagram below, labeling basic- and intermediate-level events.
2. Prob[Failure] = 1 – Prob[No Failure] = 1 – Reliability
3. Reliability of a parent event =
   -OR gate: **Product** of Reliabilities of its child events
   -AND gate: **Sum** of Reliabilities of its child events minus the **product** of Reliabilities of its child events
4. Demonstrate calculating one or more event probabilities Pr[Failure] from probabilities of basic-event failures.
5. Describe tasks that will apply the above approach to the topic of your semester report.

# 2.6 – Scenario Development


Scenario Development: Worst-Case Attack Chain
Smart Camera Compromised
Lateral Movement to Smart Lock
Full Network Access
Manipulation of Thermostat Settings
Privacy Breach and Physical Risk

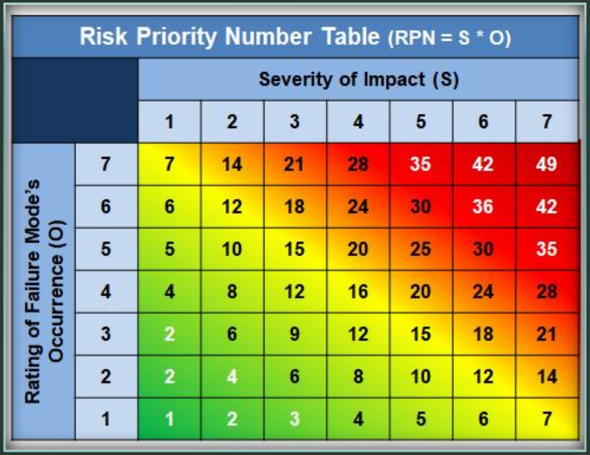
**This subtask will** develop worst-case cybersecurity breach scenarios for smart home environments, describing how small compromises (such as an infected smart camera) could escalate into system-wide incidents (like full smart home control loss). Each scenario will model a realistic chain of cascading effects and the potential damages associated.

**The elements of this subtask are** creating attack scenarios from initial infection points, mapping out cascading effects across interconnected devices, and estimating the impacts in terms of privacy loss, financial cost, and physical risk.

**The deliverables of this subtask are** detailed worst-case scenario descriptions, including attack flow diagrams and qualitative/quantitative risk assessments for each modeled event chain.

# 2.7 – Single-Point Failure Scenario Modeling

- **This subtask will** simulate single-point failures (e.g., a single device compromise) without cascades, modeling isolated attack scenarios to better compare against cascading failures.
  **The elements of this subtask are** selecting isolated attack examples, mapping device-specific impacts only, and estimating standalone risks.
  **The deliverable of this subtask is** a **Single-Point Failure Risk Table**.



Risk Priority Number Table (RPN = S * O)

| | | Severity of Impact (S) | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Rating of Failure Mode's Occurrence (O) | 7 | 7 | 14 | 21 | 28 | 35 | 42 | 49 |
| | 6 | 6 | 12 | 18 | 24 | 30 | 36 | 42 |
| | 5 | 5 | 10 | 15 | 20 | 25 | 30 | 35 |
| | 4 | 4 | 8 | 12 | 16 | 20 | 24 | 28 |
| | 3 | 2 | 6 | 9 | 12 | 15 | 18 | 21 |
| | 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 |
| | 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

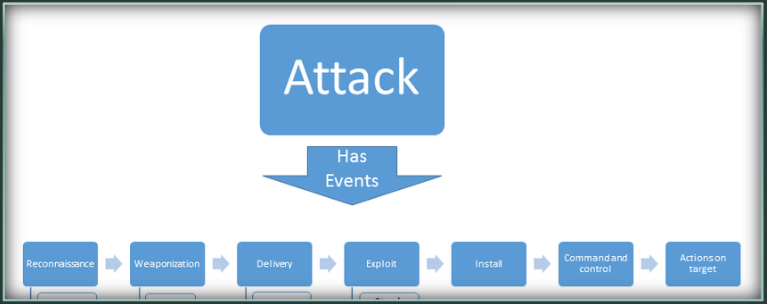
https://www.outsourcedpharma.com/doc/fmea-vs-system-risk-structures-srs-which-is-more-useful-0001

# 2.8 – Cross-Device Attack Chains

- **This subtask will** model multi-device attack chains where a compromise spreads laterally across device types (e.g., camera ➔ lock ➔ hub ➔ thermostat).

  **The elements of this subtask are** building multi-hop attack scenarios, mapping lateral device movements, and calculating likelihoods for each chain.

  **The deliverable of this subtask is** an **Attack Chain Diagram**.



## Risk Quantification and System Analysis

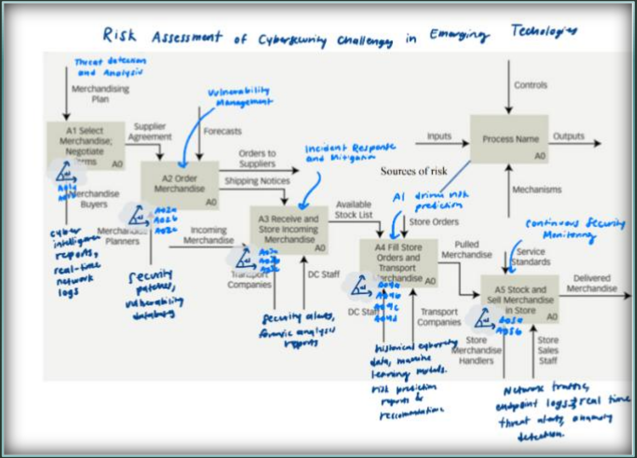
# Task 3

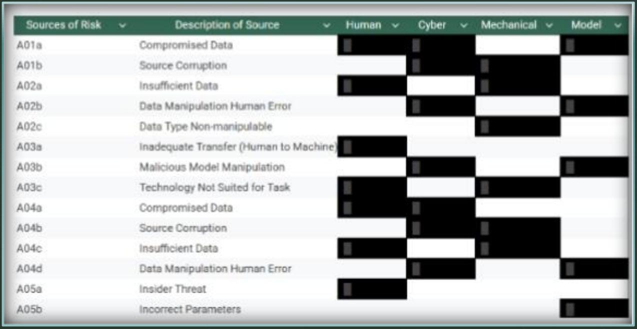
# 3.1 – Business Process Decision Map (IDEF0)

**This subtask will** model the cybersecurity decision-making workflows within the smart home IoT environment using IDEF0 diagramming. The diagram will define how smart home security actions (like isolation, patching, alert escalation) are triggered, controlled, and executed across devices and systems.

**The elements of this subtask are** identifying key cybersecurity decision processes, mapping inputs (e.g., IDS alerts), outputs (e.g., device lockdowns), controls (e.g., security policies), and resources (e.g., firmware update services) for each decision point.

**The deliverable of this subtask is** an **IDEF0 Business Process Map** showing how smart home cybersecurity decisions flow from detection to mitigation.


Risk Assessment of Cybersecurity Challenges in Emerging Technologies
Threat detection and Analysis
Merchandising Plan
Vulnerability Management
Forecasts
Supplier Agreement
A1 Select Merchandise; Negotiate Terms A0
A2 Order Merchandise A0
Orders to Suppliers
Shipping Notices
Incident Response and Mitigation
Inputs
Process Name A0
Outputs
Controls
Sources of risk
Mechanisms
A01a A01b
Merchandise Buyers
A02a A02b A02c
Merchandise Planners
Incoming Merchandise
A3 Receive and Store Incoming Merchandise A0
A03a A03b A03c
Available Stock List
AI driven risk prediction
Store Orders
A4 Fill Store Orders and Transport Merchandise A0
A04a A04b A04c A04d
Pulled Merchandise
Continuous Security Monitoring
Service Standards
A5 Stock and Sell Merchandise in Store A0
A05a A05b
Delivered Merchandise
cyber intelligence reports, real-time network logs
security patches, vulnerability database
Transport Companies
DC Staff
security alerts, forensic analysis reports
DC Staff
Transport Companies
historical cybersecurity data, machine learning models. risk prediction reports & reccomendations
Store Merchandise Handlers
Store Sales Staff
Network traffic, endpoint logs & real time threat alerts, anomaly detection.



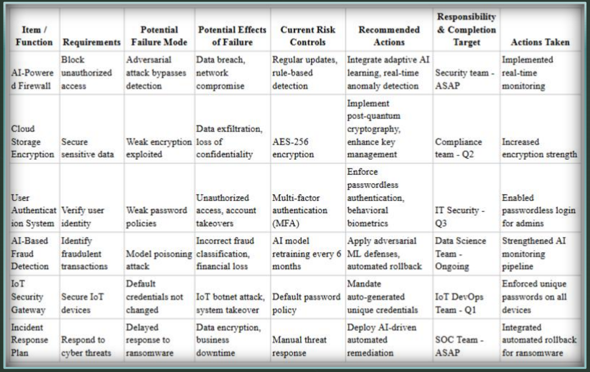
| Sources of Risk | Description of Source | Human | Cyber | Mechanical | Model |
|---|---|---|---|---|---|
| A01a | Compromised Data | ■ | ■ |  | ■ |
| A01b | Source Corruption |  | ■ | ■ |  |
| A02a | Insufficient Data | ■ |  | ■ |  |
| A02b | Data Manipulation Human Error |  | ■ |  | ■ |
| A02c | Data Type Non-manipulable |  |  | ■ |  |
| A03a | Inadequate Transfer (Human to Machine) | ■ |  |  |  |
| A03b | Malicious Model Manipulation |  | ■ |  | ■ |
| A03c | Technology Not Suited for Task | ■ |  | ■ |  |
| A04a | Compromised Data | ■ | ■ |  |  |
| A04b | Source Corruption |  | ■ | ■ |  |
| A04c | Insufficient Data | ■ |  | ■ |  |
| A04d | Data Manipulation Human Error |  | ■ |  | ■ |
| A05a | Insider Threat | ■ |  |  |  |
| A05b | Incorrect Parameters |  |  |  | ■ |

# 3.2 – Failure Modes and Effects (FMEA) for IoT

**This subtask will** perform a Failure Modes and Effects Analysis (FMEA) on critical smart home IoT devices. Each device will be evaluated for possible cybersecurity-related failure modes (e.g., credential leak, firmware tampering), and the impacts, severity, and detection likelihood will be scored to prioritize the highest-risk components for action.

**The elements of this subtask are** listing key devices, describing possible failure modes, evaluating causes and effects, scoring Severity (S), Occurrence (O), and Detection (D), and calculating Risk Priority Numbers (RPNs).

**The deliverable of this subtask is** an **FMEA Table** identifying and prioritizing device-specific cyber vulnerabilities in the smart home.



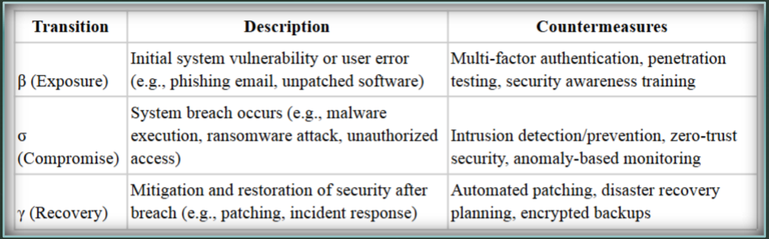
| Item / Function | Requirements | Potential Failure Mode | Potential Effects of Failure | Current Risk Controls | Recommended Actions | Responsibility & Completion Target | Actions Taken |
|---|---|---|---|---|---|---|---|
| AI-Powered Firewall | Block unauthorized access | Adversarial attack bypasses detection | Data breach, network compromise | Regular updates, rule-based detection | Integrate adaptive AI learning, real-time anomaly detection | Security team - ASAP | Implemented real-time monitoring |
| Cloud Storage Encryption | Secure sensitive data | Weak encryption exploited | Data exfiltration, loss of confidentiality | AES-256 encryption | Implement post-quantum cryptography, enhance key management | Compliance team - Q2 | Increased encryption strength |
| User Authentication System | Verify user identity | Weak password policies | Unauthorized access, account takeovers | Multi-factor authentication (MFA) | Enforce passwordless authentication, behavioral biometrics | IT Security - Q3 | Enabled passwordless login for admins |
| AI-Based Fraud Detection | Identify fraudulent transactions | Model poisoning attack | Incorrect fraud classification, financial loss | AI model retraining every 6 months | Apply adversarial ML defenses, automated rollback | Data Science Team - Ongoing | Strengthened AI monitoring pipeline |
| IoT Security Gateway | Secure IoT devices | Default credentials not changed | IoT botnet attack, system takeover | Default password policy | Mandate auto-generated unique credentials | IoT DevOps Team - Q1 | Enforced unique passwords on all devices |
| Incident Response Plan | Respond to cyber threats | Delayed response to ransomware | Data encryption, business downtime | Manual threat response | Deploy AI-driven automated remediation | SOC Team - ASAP | Integrated automated rollback for ransomware |

# 3.3 – SEIRS Model for Cyber Infection and Recovery

**This subtask will** apply a SEIRS epidemiological model (Susceptible-Exposed-Infected-Recovered-Susceptible) to simulate how malware infections spread, recover, and possibly reoccur among smart home IoT devices. The model will visualize infection rates, recovery rates, and re-susceptibility cycles over time.

**The elements of this subtask are** defining device infection states, setting transition rates (infection, exposure, recovery, and immunity loss), creating differential equations for state changes, and plotting device infection/recovery curves.

**The deliverable of this subtask is** a **SEIRS State Transition Diagram** and **Infection/Recovery Curves** modeling cyber infection dynamics in the smart home.



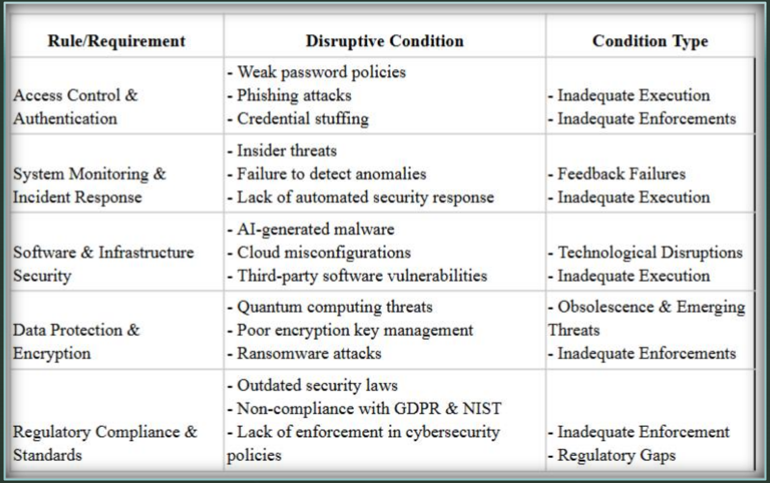
| Transition | Description | Countermeasures |
|---|---|---|
| β (Exposure) | Initial system vulnerability or user error (e.g., phishing email, unpatched software) | Multi-factor authentication, penetration testing, security awareness training |
| σ (Compromise) | System breach occurs (e.g., malware execution, ransomware attack, unauthorized access) | Intrusion detection/prevention, zero-trust security, anomaly-based monitoring |
| γ (Recovery) | Mitigation and restoration of security after breach (e.g., patching, incident response) | Automated patching, disaster recovery planning, encrypted backups |

# 3.4 – STAMP Modeling of Disruptive Conditions

**This subtask will** model smart home system vulnerabilities using Systems-Theoretic Accident Model and Processes (STAMP) analysis. It will map unsafe control actions, inadequate feedback loops, and missing constraints that could allow cyber disruptions to escalate.

**The elements of this subtask are** identifying unsafe control actions (e.g., a smart lock accepting unverified updates), mapping control structure diagrams (controllers, actuators, sensors), and describing pathways from control errors to system losses.

**The deliverable of this subtask is** a **STAMP Control Structure Diagram** and a list of unsafe control actions for the smart home system.



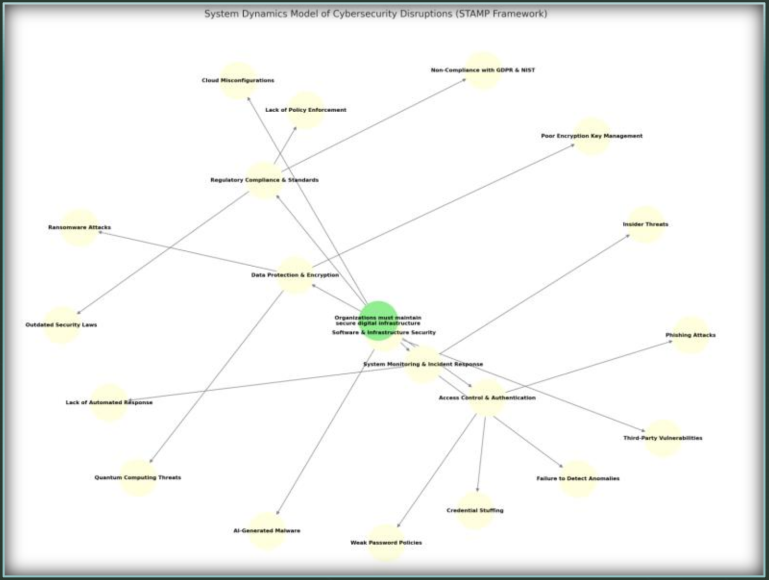
| Rule/Requirement | Disruptive Condition | Condition Type |
|---|---|---|
| Access Control & Authentication | - Weak password policies<br>- Phishing attacks<br>- Credential stuffing | - Inadequate Execution<br>- Inadequate Enforcements |
| System Monitoring & Incident Response | - Insider threats<br>- Failure to detect anomalies<br>- Lack of automated security response | - Feedback Failures<br>- Inadequate Execution |
| Software & Infrastructure Security | - AI-generated malware<br>- Cloud misconfigurations<br>- Third-party software vulnerabilities | - Technological Disruptions<br>- Inadequate Execution |
| Data Protection & Encryption | - Quantum computing threats<br>- Poor encryption key management<br>- Ransomware attacks | - Obsolescence & Emerging Threats<br>- Inadequate Enforcements |
| Regulatory Compliance & Standards | - Outdated security laws<br>- Non-compliance with GDPR & NIST<br>- Lack of enforcement in cybersecurity policies | - Inadequate Enforcement<br>- Regulatory Gaps |

# 3.5 – Cyber Risk Feedback Loop Modeling

**This subtask will** build system dynamics models showing positive and negative feedback loops that influence cybersecurity risk over time (e.g., successful attacks increase risk exposure, while patching reduces it). It will visualize how system vulnerabilities evolve dynamically, not just statically.

**The elements of this subtask are** defining feedback variables (e.g., vulnerability levels, patch rates, attack sophistication), constructing causal loop diagrams, and simulating feedback-driven risk behavior over time.

**The deliverable of this subtask is** a **System Dynamics Feedback Loop Diagram** showing reinforcing and balancing loops within smart home cybersecurity.

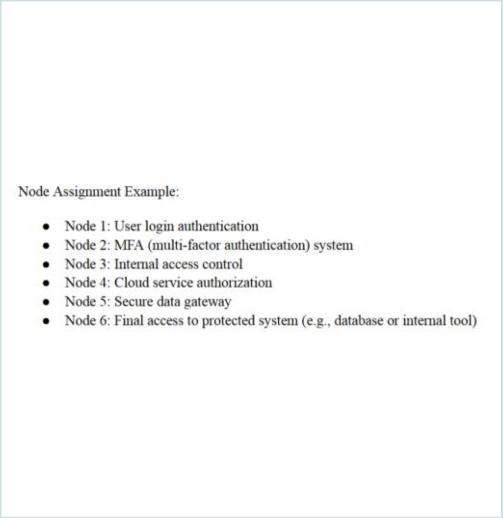

System Dynamics Model of Cybersecurity Disruptions (STAMP Framework)
Cloud Misconfigurations
Non-Compliance with GDPR & NIST
Lack of Policy Enforcement
Poor Encryption Key Management
Regulatory Compliance & Standards
Ransomware Attacks
Insider Threats
Data Protection & Encryption
Outdated Security Laws
Organizations must maintain secure digital infrastructure
Software & Infrastructure Security
Phishing Attacks
System Monitoring & Incident Response
Lack of Automated Response
Access Control & Authentication
Third-Party Vulnerabilities
Quantum Computing Threats
Failure to Detect Anomalies
Credential Stuffing
AI-Generated Malware
Weak Password Policies

# 3.6 – Network Flow Reliability Analysis

**This subtask will** model the reliability of smart home device communications under cyberattack conditions using network flow analysis. It will assess how disruptions to key network nodes (e.g., smart hubs) impact the ability of devices to communicate securely and reliably.

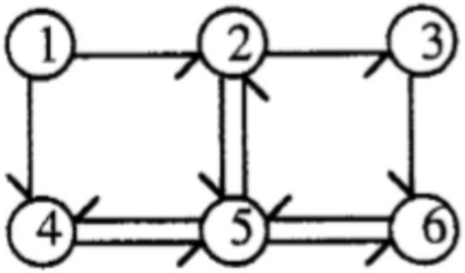
**The elements of this subtask are** mapping smart home device communication graphs, assigning link reliability probabilities, calculating minimum cuts and flow capacity, and evaluating network resilience metrics.

**The deliverable of this subtask is** a **Network Reliability Diagram** and **Flow Analysis Table** quantifying how resilient the smart home network remains under attack scenarios.



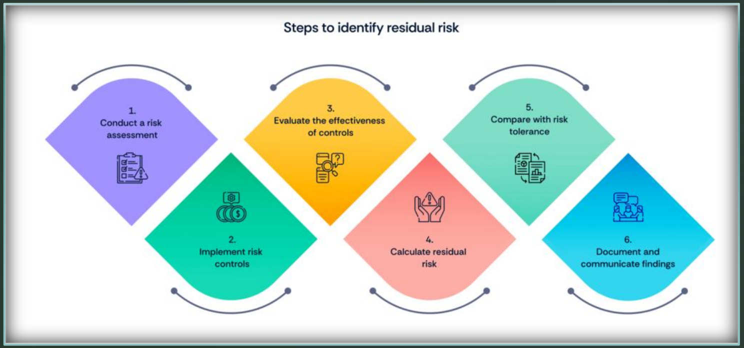
Node Assignment Example:

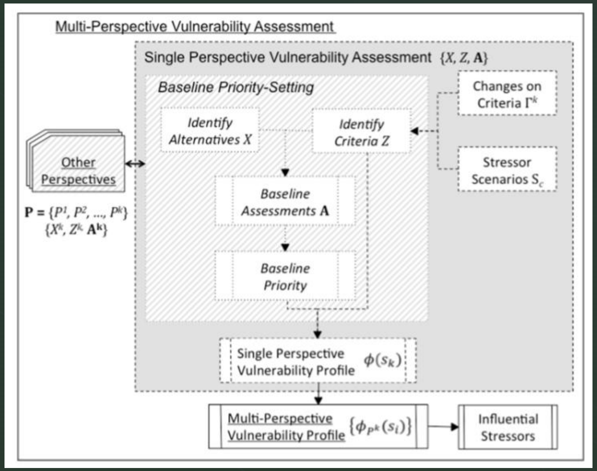
- Node 1: User login authentication
- Node 2: MFA (multi-factor authentication) system
- Node 3: Internal access control
- Node 4: Cloud service authorization
- Node 5: Secure data gateway
- Node 6: Final access to protected system (e.g., database or internal tool)



# 3.7: Quantifying Residual Risk After Resilience Strategies

- **This subtask will** calculate the "residual risk" levels for smart home devices after deploying selected cybersecurity strategies (e.g., IDS, MFA).
  **The elements of this subtask are** comparing pre- and post-mitigation risk scores, calculating percentage risk reduction, and identifying remaining vulnerabilities.
  **The deliverable of this subtask is** a **Residual Risk Comparison Flow Chart**.

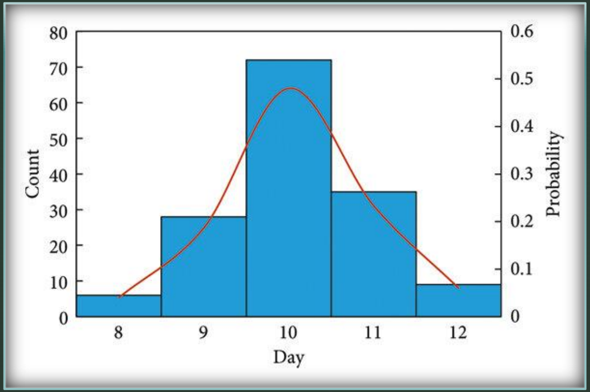

Steps to identify residual risk
1. Conduct a risk assessment
2. Implement risk controls
3. Evaluate the effectiveness of controls
4. Calculate residual risk
5. Compare with risk tolerance
6. Document and communicate findings


Multi-Perspective Vulnerability Assessment
Single Perspective Vulnerability Assessment {X, Z, A}
Baseline Priority-Setting
Changes on Criteria Γ^k
Identify Alternatives X
Identify Criteria Z
Other Perspectives
Stressor Scenarios S_c
Baseline Assessments A
P = {P^1, P^2, ..., P^k}
{X^k, Z^k, A^k}
Baseline Priority
Single Perspective Vulnerability Profile φ(s_k)
Multi-Perspective Vulnerability Profile {φ_{P^k}(s_i)}
Influential Stressors

https://www.scrut.io/post/ultimate-guide-to-residue-risk

# 3.8: Probability Distributions for Recovery Times

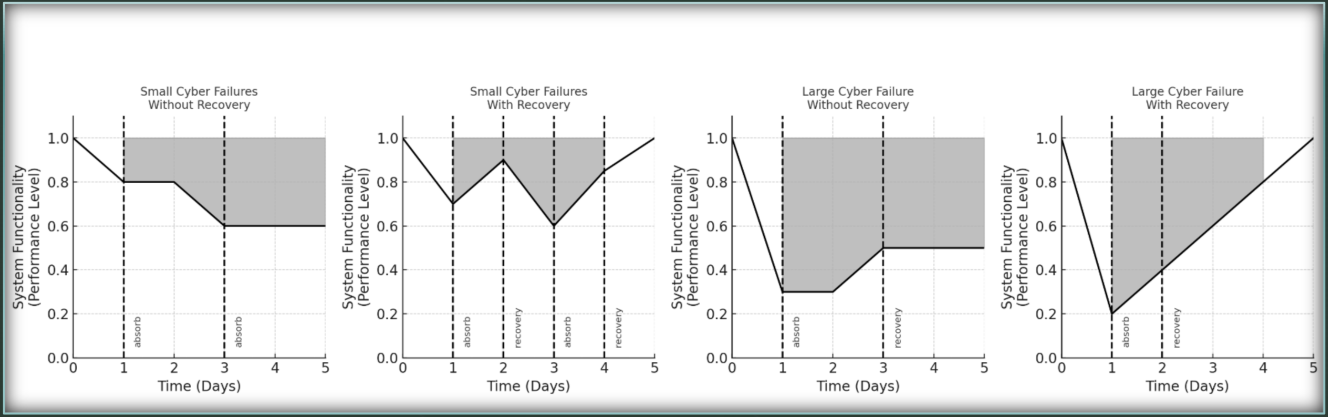
- **This subtask will** build probability distributions for how quickly different types of smart home devices recover from cyber incidents, incorporating uncertainty into resilience planning.
  **The elements of this subtask are** defining recovery event distributions, fitting probability models (e.g., normal, exponential), and graphing cumulative recovery probabilities.
  **The deliverable of this subtask is** a **Recovery Time Probability Distribution Graph**.



Resilience Modeling and Optimization

# Task 4

# 4.1 – Recovery Time vs Damage Resilience Curves



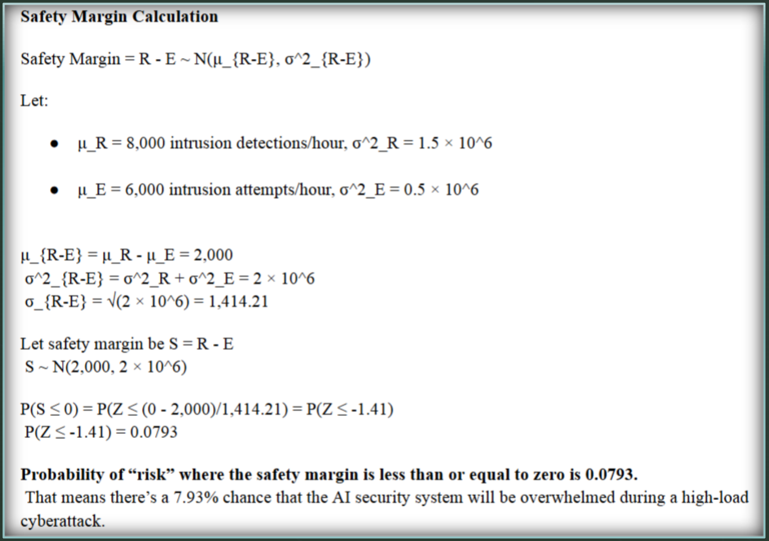
**This subtask will** model how different recovery times after a cybersecurity attack impact overall damage levels in smart home IoT environments. It will create resilience curves that show how faster recovery reduces financial, privacy, and physical damages.
**The elements of this subtask are** defining time-to-recovery intervals (e.g., immediate response, 24 hours, 48 hours), estimating damage levels associated with each interval, plotting resilience curves showing recovery vs loss impact, and analyzing thresholds for unacceptable damage.
**The deliverable of this subtask is** a **Resilience Curve Graph** showing recovery time versus system damage for smart homes.

# 4.2 – Load vs Resistance Margin Estimation

**This subtask will** estimate the safety margin between the load (attack severity) and resistance (device/system ability to withstand attacks) for key smart home IoT components. It will help determine how close systems operate to failure under normal and adversarial conditions.

**The elements of this subtask are** defining load distributions (threat severity), modeling resistance distributions (security strength), calculating probability of exceedance (when load > resistance), and estimating risk margins.

**The deliverable of this subtask is** a **Load-Resistance Distribution Plot** and calculated safety margins for critical devices.



**Safety Margin Calculation**

Safety Margin = R - E ~ N(μ_{R-E}, σ^2_{R-E})

Let:

- μ_R = 8,000 intrusion detections/hour, σ^2_R = 1.5 × 10^6
- μ_E = 6,000 intrusion attempts/hour, σ^2_E = 0.5 × 10^6

μ_{R-E} = μ_R - μ_E = 2,000

σ^2_{R-E} = σ^2_R + σ^2_E = 2 × 10^6

σ_{R-E} = √(2 × 10^6) = 1,414.21

Let safety margin be S = R - E

S ~ N(2,000, 2 × 10^6)

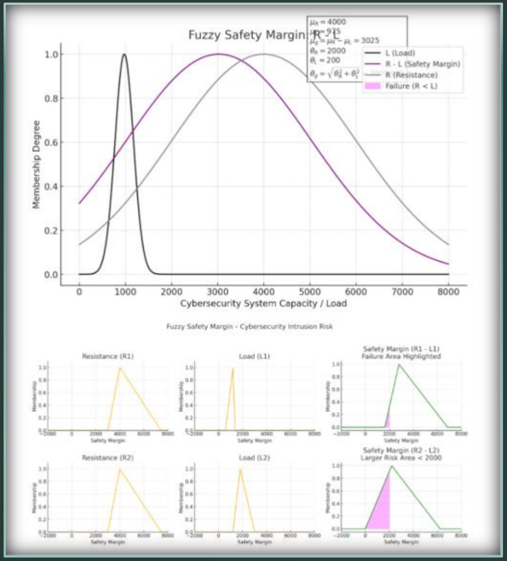
P(S ≤ 0) = P(Z ≤ (0 - 2,000)/1,414.21) = P(Z ≤ -1.41)

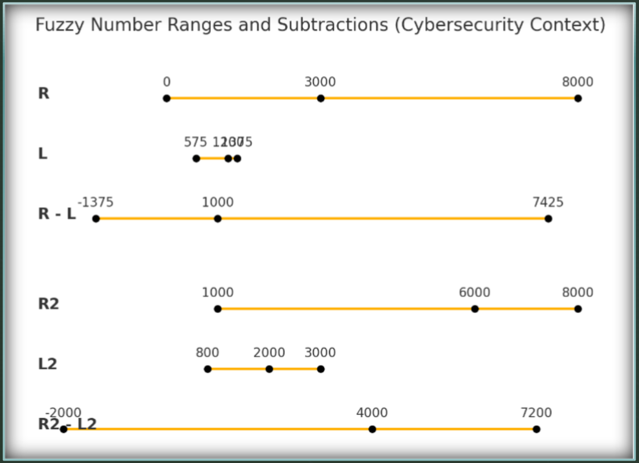
P(Z ≤ -1.41) = 0.0793

**Probability of "risk" where the safety margin is less than or equal to zero is 0.0793.**
That means there's a 7.93% chance that the AI security system will be overwhelmed during a high-load cyberattack.

# 4.3 – Fuzzy Safety Margin Assessment

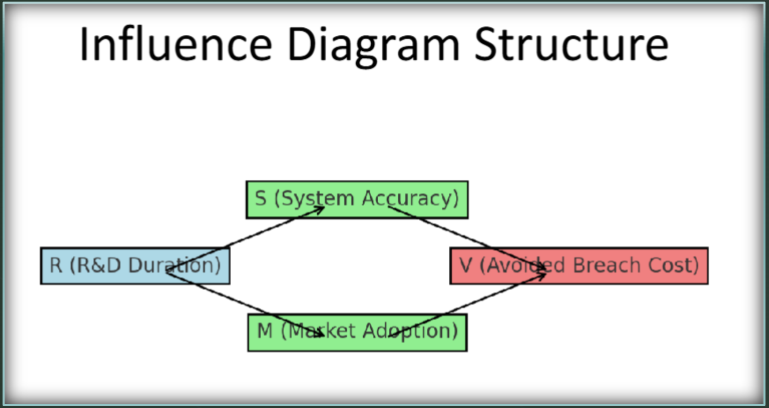
**This subtask will** use fuzzy logic modeling to assess uncertainty in smart home cybersecurity safety margins. Since exact risk numbers are hard to predict (due to device variation, unknown threats, etc.), fuzzy membership functions will be used to estimate safe vs unsafe system conditions. **The elements of this subtask are** defining fuzzy sets for load and resistance, creating membership functions (e.g., "high risk", "medium risk", "low risk"), applying fuzzy rules for assessing overall system resilience, and graphically representing uncertainty zones. **The deliverable of this subtask is** a **Fuzzy Logic Risk Assessment Diagram** showing system risk membership regions.



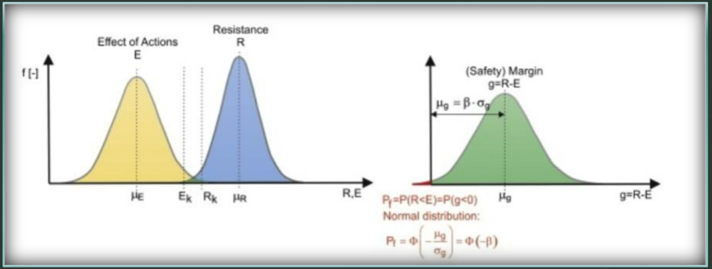


# 4.4 – Influence Diagram Decision Mapping

**This subtask will** build an influence diagram mapping the relationships between cybersecurity actions (like patching or isolating devices) and outcomes (like reduced risk or faster recovery) in smart homes. This will help visualize key decision variables, uncertainties, and resulting outcomes.
**The elements of this subtask are** identifying decision nodes (e.g., apply firmware update?), chance nodes (e.g., patch success probability), and outcome nodes (e.g., reduced breach risk), connecting nodes logically, and labeling node influences.
**The deliverable of this subtask is** an **Influence Diagram** showing how smart home cybersecurity decisions impact risk outcomes.



# 4.5 – AI-Based Intrusion Detection Simulation Results

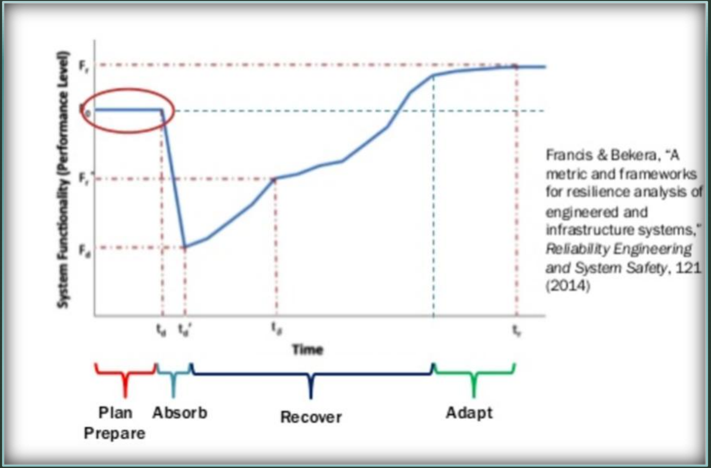


- **This subtask will** simulate the effect of implementing an AI-based Intrusion Detection System (IDS) on smart home networks, tracking detection rates and false positives.

  **The elements of this subtask are** setting detection thresholds, simulating AI learning curves, plotting detection vs false positive rates.

  **The deliverable of this subtask is** an **IDS Detection vs False Positive Graph**.

# 4.6 – Device Redundancy Planning



Francis & Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," *Reliability Engineering and System Safety*, 121 (2014)

**This subtask will model system resilience by analyzing how smart home cybersecurity infrastructure recovers from disruptions over time, with and without device redundancy.** Using resilience curve modeling, we will compare system performance degradation and recovery following a simulated attack or failure event.

The curve illustrates how quickly a system regains functionality based on the availability of backup devices, automated response systems, and recovery protocols. The **area under the curve** represents total system resilience, while the lowest point reflects the system's vulnerability or performance loss during failure.

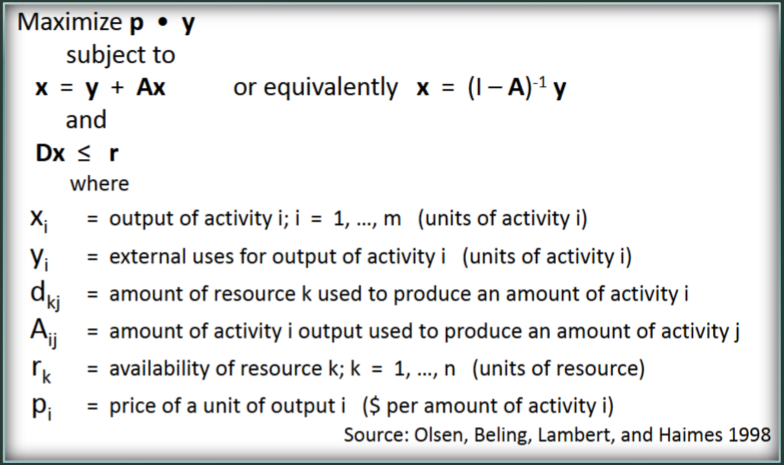
**The elements of this subtask are** identifying critical devices (e.g., smart locks, hubs), mapping primary and backup roles, and evaluating recovery time with and without redundancy.

**The deliverable of this subtask is a Resilience Curve Diagram**, showing performance over time and demonstrating how redundancy strategies shorten downtime and reduce long-term impact.

Failure Simulation and Recovery Dynamics

# Task 5

## 5.1 – Resource Dependency Simulation (Leontief Modeling)



Maximize $\mathbf{p} \bullet \mathbf{y}$

subject to

$\mathbf{x} = \mathbf{y} + \mathbf{A}\mathbf{x}$ or equivalently $\mathbf{x} = (\mathrm{I} - \mathbf{A})^{-1}\,\mathbf{y}$

and

$\mathbf{D}\mathbf{x} \leq \mathbf{r}$

where

$x_i$ = output of activity i; i = 1, ..., m (units of activity i)

$y_i$ = external uses for output of activity i (units of activity i)

$d_{kj}$ = amount of resource k used to produce an amount of activity i

$A_{ij}$ = amount of activity i output used to produce an amount of activity j

$r_k$ = availability of resource k; k = 1, ..., n (units of resource)

$p_i$ = price of a unit of output i ($ per amount of activity i)

Source: Olsen, Beling, Lambert, and Haimes 1998

**This subtask will** simulate resource and service dependencies within the smart home IoT ecosystem using an Input-Output (Leontief) modeling approach. It will analyze how the disruption of one device or service (e.g., smart hub failure) cascades through dependent devices (e.g., locks, cameras, thermostats) and affects overall system operations.

**The elements of this subtask are** mapping device interdependencies, creating an input-output matrix, applying Leontief inverse calculations to measure total disruption impacts, and identifying critical dependency points.

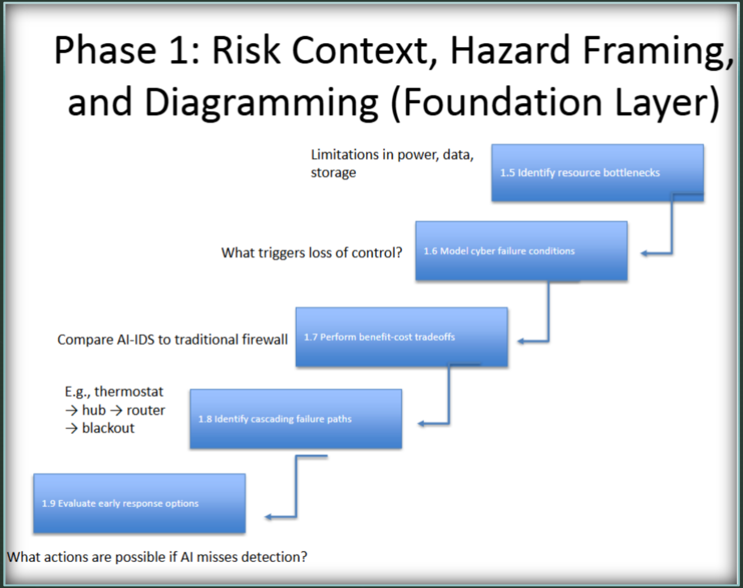
**The deliverable of this subtask is** a **Resource Dependency Matrix** and a **Disruption Simulation Output Table** showing how failures propagate across smart home devices.

# 5.2 – Cascading Cyber Failures Simulation

**This subtask will** simulate how cyber failures cascade through a smart home network over time, using system dynamics or agent-based simulation techniques. It will visualize how an initial breach can lead to secondary failures (e.g., smart lock hack ➔ alarm system compromise ➔ surveillance disabled ➔ total control loss).

**The elements of this subtask are** setting up initial breach conditions, defining device/device interaction rules, running forward simulation steps, and plotting cascading impacts by time or device tier.

**The deliverable of this subtask is** a **Cascade Failure Simulation Diagram** or **Timeline Graph** showing the spread of device failures from initial compromise to full system disruption.



Phase 1: Risk Context, Hazard Framing, and Diagramming (Foundation Layer)

Limitations in power, data, storage

1.5 Identify resource bottlenecks

What triggers loss of control?

1.6 Model cyber failure conditions

Compare AI-IDS to traditional firewall

1.7 Perform benefit-cost tradeoffs

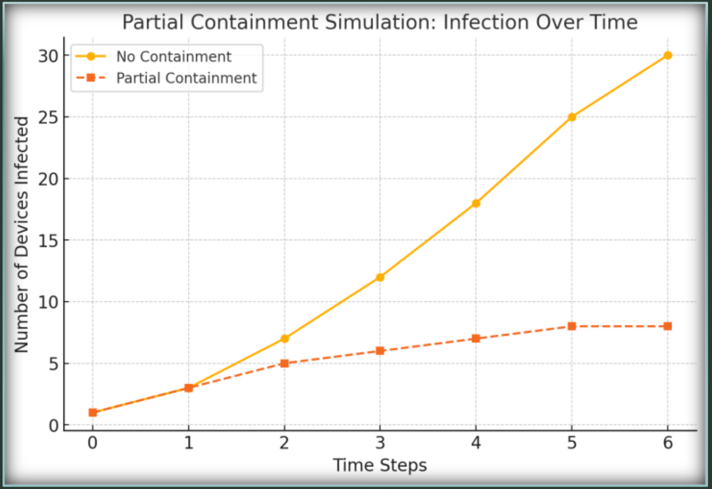
E.g., thermostat
→ hub → router
→ blackout

1.8 Identify cascading failure paths

1.9 Evaluate early response options

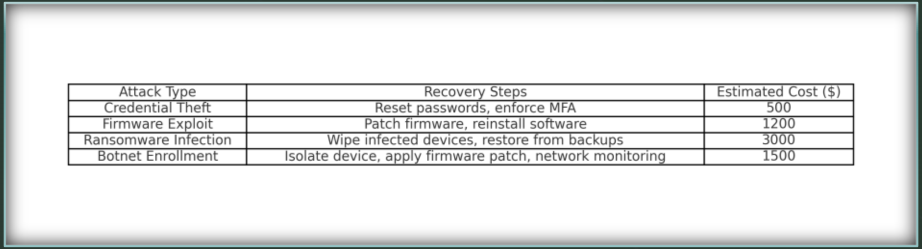
What actions are possible if AI misses detection?

# 5.3 – Partial Containment Simulation



- **This subtask will** simulate partial containment scenarios where a cyberattack is detected late but limited action reduces full compromise.
  **The elements of this subtask are** setting partial containment points (e.g., isolate hub after 2 devices infected), simulating risk trajectory, and comparing outcomes to full cascades.
  **The deliverable of this subtask is** a **Partial Containment Timeline Graph**.

# 5.4 – Recovery Cost Estimation



| Attack Type | Recovery Steps | Estimated Cost ($) |
|---|---|---|
| Credential Theft | Reset passwords, enforce MFA | 500 |
| Firmware Exploit | Patch firmware, reinstall software | 1200 |
| Ransomware Infection | Wipe infected devices, restore from backups | 3000 |
| Botnet Enrollment | Isolate device, apply firmware patch, network monitoring | 1500 |

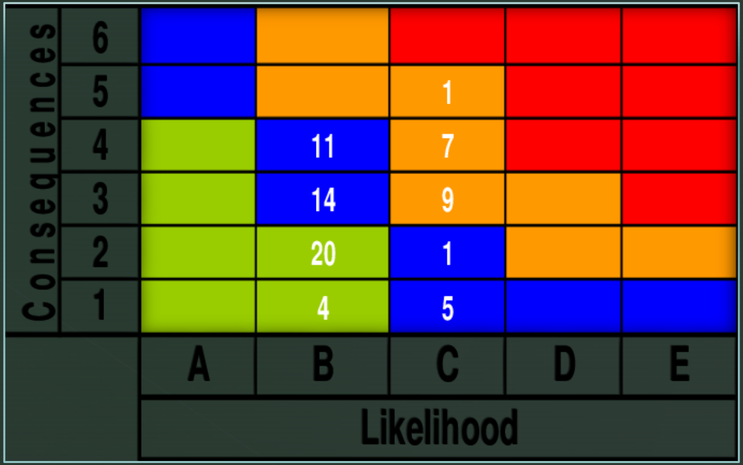
- **This subtask will** estimate financial and operational costs associated with recovery from different levels of smart home cyberattacks.
  **The elements of this subtask are** modeling direct costs (device resets, firmware patches) and indirect costs (downtime, privacy breaches) for different scenarios.
  **The deliverable of this subtask is** a **Cost Estimation Table for Recovery**.

# Project Synthesis and Recommendations

# Task 6

# 6.1 – Overall System Resilience Heatmap

- **This subtask will** create a final resilience heatmap showing the overall risk exposure levels of different smart home IoT devices after applying all modeled cybersecurity strategies. Devices will be color-coded based on their residual risk (e.g., high, medium, low).
  **The elements of this subtask are** aggregating resilience scores across devices, applying color thresholds for risk levels, visually plotting device categories by final risk, and annotating key vulnerabilities.
  **The deliverable of this subtask is** a **Systemwide Resilience Heatmap** summarizing final smart home cybersecurity standing.

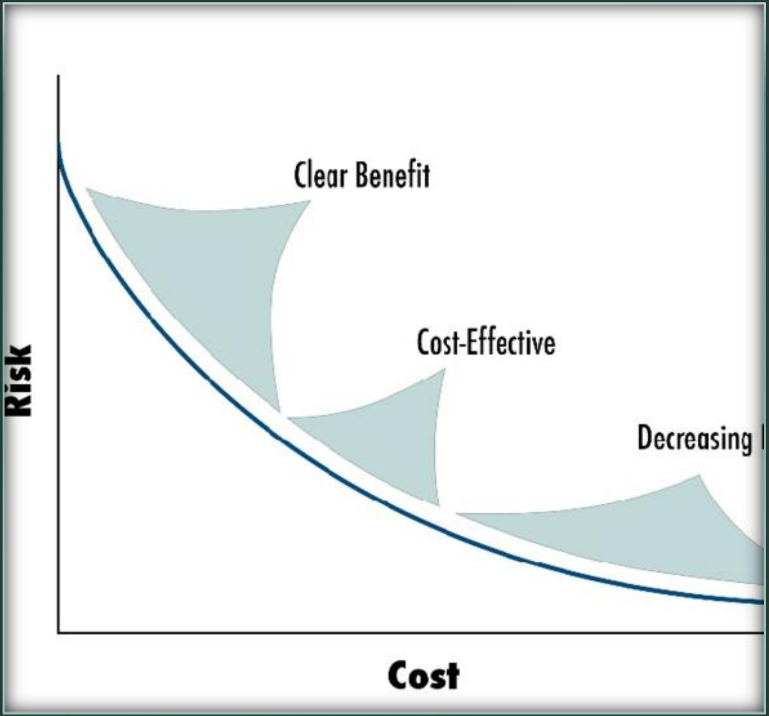


| | | | | | | |
|---|---|---|---|---|---|---|
| Consequences | 6 | 🟦 | 🟧 | 🟥 | 🟥 | 🟥 |
| | 5 | 🟦 | 🟧 | 🟧 1 | 🟥 | 🟥 |
| | 4 | 🟩 | 🟦 11 | 🟧 7 | 🟥 | 🟥 |
| | 3 | 🟩 | 🟦 14 | 🟧 9 | 🟧 | 🟥 |
| | 2 | 🟩 | 🟩 20 | 🟦 1 | 🟧 | 🟧 |
| | 1 | 🟩 | 🟩 4 | 🟦 5 | 🟦 | 🟦 |
| | | A | B | C | D | E |
| | | Likelihood | | | | |

https://www.researchgate.net/figure/Example-of-a-risk-heat-map-8-for-the-IPS-as-the-outcome-of-this-step_fig3_312606481

# 6.2 – Cyber Resilience vs Cost Efficiency Tradeoff Plot

- **This subtask will** graph the tradeoff between increasing cybersecurity resilience (via technologies like AI-based IDS or blockchain updates) versus their financial cost. It will highlight diminishing returns zones where higher investments produce minimal security gains. **The elements of this subtask are** plotting cost on one axis, resilience improvement on the other axis, identifying tradeoff curves, and recommending optimal investment points. **The deliverable of this subtask is** a **Resilience vs Cost Tradeoff Graph** showing ideal balance points between security and expense.



https://www.researchgate.net/figure/Conceptual-diagram-of-the-cost-of-buying-down-risk-in-cyber-systems_fig1_325461632

# Conclusion

AI-driven risk analysis is rapidly transforming the cybersecurity outlook for IoT-enabled smart homes. Through intelligent monitoring and adaptive learning, AI systems can detect cybersecurity threats that would likely evade traditional methods, significantly enhancing the protection of personal data and the safety of home automation systems [1][2].

Our research indicates that leveraging machine learning for **anomaly detection** and **predictive analytics** helps mitigate core IoT security concerns, including unauthorized device access, privacy breaches, and botnet recruitment [1][2]. Moreover, AI's capacity to recognize and respond to evolving attack patterns in real time enables **a dynamic defense posture**—critical for protecting households against increasingly sophisticated cyber threats.

While AI offers transformative capabilities, it is not a complete solution on its own. Vulnerabilities such as **firmware exploits** or **zero-day flaws** still require complementary safeguards like robust device patching protocols and secure hardware design [1]. However, the trajectory in both industry and academia is clear: artificial intelligence will continue to play a central role in fortifying smart home ecosystems [2].

For **SmartSecure Systems**, this integrative framework demonstrates how AI-driven risk analysis can be operationalized to deliver real-time protection, customer trust, and long-term system resilience. By combining advanced analytics with proactive monitoring and tailored risk mitigation strategies, SmartSecure can offer homeowners a **security solution that is intelligent, responsive, and future-ready**—positioning the company as a leader in residential cybersecurity innovation.

[1] https://doi.org/10.3390/electronics12183958
[2] https://doi.org/10.3389/fdata.2024.1402745

# Next Steps

- **Research Emerging Threats**
  Investigate device authentication bypasses and cloud-based attack vectors [1][2]
  → *Helps SmartSecure stay ahead of evolving vulnerabilities*

- **Expand Real-World Testing**
  Deploy AI systems in diverse live smart home environments [2]
  → *Validates performance and improves real-time adaptation*

- **Develop Industry Standards**
  Contribute to best practices for data logging and system interoperability [5]
  → *Ensures SmartSecure solutions are scalable and compliant*

- **Enhance Explainability of AI**
  Improve clarity and transparency of alerts for users and professionals [4]
  → *Boosts user trust and actionable response*

- **Scale to Other IoT Sectors**
  Apply lessons from smart homes to smart cities and healthcare IoT [2][3]
  → *Positions SmartSecure as a leader in broader cybersecurity markets*

[1] https://doi.org/10.3390/electronics12183958
[2] https://doi.org/10.3389/fdata.2024.1402745
[4] https://doi.org/10.3390/s22052017
[5] https://www.oberlo.com/statistics/smart-home-statistics

# Next Steps

- By executing the six-phase AI-driven risk analysis framework outlined in the Gantt chart, SmartSecure Systems will establish itself as a leader in next-generation smart home cybersecurity. Each phase strategically integrates modeling, scenario planning, and resilience assessment to deliver targeted, data-driven protection against evolving IoT threats. Through quantification of residual risk and simulation of real-world disruptions, SmartSecure can minimize financial loss, optimize resource deployment, and build customer trust. Additionally, by incorporating explainability and real-time feedback into its AI models, SmartSecure ensures a secure and intuitive experience for homeowners from initial deployment through long-term use.

# References

1. **AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023).** *Cybersecurity Risk Analysis in the IoT: A Systematic Review*. Electronics, 12(18), 3958. https://doi.org/10.3390/electronics12183958

2. **Radanliev, P., De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R., & Ani, U. (2024).** *AI Security and Cyber Risk in IoT Systems*. Frontiers in Big Data, 7, Article 1402745. https://doi.org/10.3389/fdata.2024.1402745

3. **Mazhar, T., Talpur, D. B., et al. (2023).** *Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence*. Brain Sciences, 13(4), 683. https://doi.org/10.3390/brainsci13040683

4. **Koroniotis, N., Moustafa, N., & Slay, J. (2022).** *Towards a New Generation of IoT Cybersecurity Framework: AI-driven Risk Assessment*. Sensors, 22(5), 2017. https://doi.org/10.3390/s22052017

5. **Oberlo Research. (2024).** *US Smart Home Statistics (2019–2028)*. Retrieved from https://www.oberlo.com/statistics/smart-home-statistics

6. Lambert, J. H., Parlak, A., Cevik, S., & Karvetski, C. W. (2013). *A framework for risk-informed planning for hazardous events with distributed impacts*. Accident Analysis & Prevention, 59, 329–337.

7. Teng, S., Thekdi, S., & Lambert, J. H. (2012). *Risk-based decision making for cyber-physical systems*. Safety Science, 50(7), 1512–1520.

8. Rogerson, D., Lambert, J. H., & Linkov, I. (2012). *Scenario and multiple criteria decision analysis for climate-related risk management of transportation infrastructure*. Risk Analysis, 32(9), 1431–1447.

9. Thorisson, H., Lambert, J. H., Cardenas, J. J., & Linkov, I. (2016). *Modeling infrastructure risk due to extreme events: Influence diagrams for cyber risk planning*. Risk Analysis, 36(7), 1310–1327.

10. Tsang, H., Lambert, J. H., & Patev, R. C. (2002). *Infrastructure risk prioritization under uncertainty: An integrative approach*. Journal of Infrastructure Systems, 8(4), 131–140.

11. You, H., Lambert, J. H., Clarens, A. F., & McFarlane, B. J. (2014). *Quantifying resilience of infrastructure systems: A probabilistic approach*. IEEE Systems Journal, 8(4), 1132–1142.

12. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., et al. (2005). *Inoperability input-output model for interdependent infrastructures*. Journal of Infrastructure Systems, 11(2), 67–79.

13. Thorisson, H., & Lambert, J. H. (2017). *Risk analysis of cybersecurity and interdependent systems: Influence modeling and mitigation strategies*. Reliability Engineering & System Safety, 167, 449–456.

14. Moghadasi, M., Dehghani, S., & Fazel, M. (2024). *A system-based approach to evaluate trust in AI-assisted medical diagnosis: Case study in cardiac sarcoidosis*. International Symposium on Computer Vision (ISCV).